TUTTI I SOFTWARE MIGLIORI SPIEGATI PASSO PASSO

HACKERS

MAGAZINE.IT

FIRESHEEP
Attacco e contromisure
del plug-in in grado di bucare l'https

GRATIS!

TOP 100 BY HM
I MIGLIORI PROGRAMMI PER L'HACKER

HACKING
MULTIMEDIA
PROGRAMMING
COPY
NETWORKING
SYSTEM
WEB
P2P
SECURITY

HACKERS MAGAZINE N°64 - BIM. - ANNO 10 - 2011
€ 4,99 - DISTRIBUTORE: M-DIS DISTRIBUZIONE SPA
10064
9 771720 767009
WLF PUBLISHING

NOTIZIE, MAIL, CURIOSITÀ, TRUCCHI & SEGRETI...

DOMANDA E RISPOSTA

>SOMMARIO

TANTO SOFTWARE

Si chiude un'annata di Hackers Magazine che ha visto una grande quantità di software selezionato e distribuito attraverso l'ormai inconfondibile CD allegato alla rivista. In questo numero siamo andati davvero al limite, almeno quello fisico del supporto, infatti, abbiamo pressoché completamente occupato i 700 MB di spazio disponibile.
All'interno del supporto troverete molto del software spiegato con grande precisione dai nostri autori negli articoli contenuti in questo numero 64. Un occhio di riguardo come al solito per le sezioni dedicate alla sicurezza e all'hacking, ma anche la sezione Multimedia si presenta particolarmente ricca, con tutti gli strumenti necessari per realizzare una vera radio, un sogno di molti all'inizio degli anni '70, quando si diffuse il fenomeno delle radio libere, che è diventato ora, grazie al software open source e a internet, alla portata di tutti.

Buona lettura a tutti

La redazione

HACKERSMAGAZINE.IT
Anno 10 - N. 64 2011

Editore: WLF Publishing S.r.l
Socio Unico medi & Son S.r.l
Via Torino, 51 20063 Cernusco S/Naviglio
Tel 02924321 e fax 02/92432236

Direttore responsabile: Teresa Carsaniga

Realizzazione Editoriale: Progetti e Promozioni Srl
redazione@hackerjournal.it

Stampa: Arti Grafiche Boccia SpA (SA)

Distributore: M-DIS Distribuzione Spa
Via Cazzaniga 19 – 20123 Milano

HACKERS MAGAZINE
Pubblicazione registrata al Tribunale di Milano il 15/07/2002 con il numero 414.

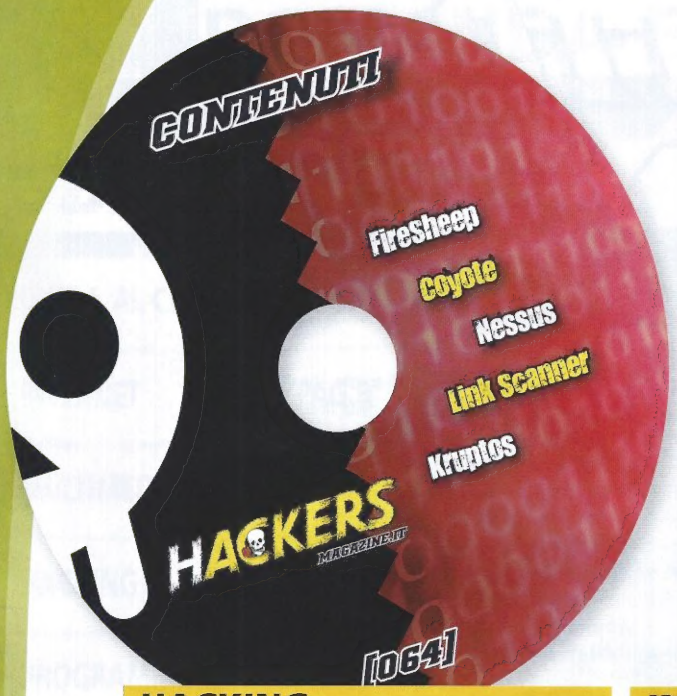
Una copia: euro 4.99

A TUTTO SPAM

Secondo un recente rapporto, la quota di spam con allegati pericolosi nel traffico di posta elettronica ha superato il 6,3% del traffico email generale. Il genere di "mailing di massa" con il maggiore aumento è quello delle finte notifiche provenienti da fonti apparentemente ufficiali, come Twitter, Facebook, WindowsLive, MySpace e diversi notissimi negozi on line. I link contenuti in queste notifiche fasulle dirottano gli utenti ad uno spammer service che scarica il backdoor Bredolab nei computer degli utenti, ed è poi usato a sua volta per scaricare vari altri Trojan.

"L'aumento del volume e della qualità di queste mailing di massa conferma l'ipotesi che gli spammer e i cybercriminali hanno iniziato ad agire all'unisono e di comune accordo per creare delle strategie d'infezione nuove e più complesse, come connettere il computer di una vittima a un Botnet inviandogli spam, per rubare i suoi dati personali e via dicendo" afferma Darya Gudkova, Head of Content Analysis & Research alla Kaspersky Lab. C'è tuttavia anche un indicatore positivo, il livello di spam generale (quindi non solo quello con allegati pericolosi) nel terzo trimestre del 2010 è calato rispetto al trimestre precedente, con una media dell'82,3%. Gli utenti hanno quindi trovato nelle proprie caselle di posta elettronica, a settembre, una quantità di spam considerevolmente inferiore rispetto al mese di agosto, con una flessione di 1,5 punti percentuali. La causa della flessione è dovuta principalmente alla chiusura di oltre 20 centri di controllo usati dal Botnet Pushdo / Cutwail, che era responsabile di circa il 10% di tutto lo spam mondiale. Questa minaccia non era solo legata all'enorme volume di spam distribuito, ma anche al suo collegamento con la diffusione di programmi particolarmente dannosi come Zbot (ZeuS) e TDSS. Quando i centri di comando del Bootnet sono stati chiusi, un enorme numero di bot ha smesso di distribuire spam, non essendo più sotto il controllo degli spammer. Un'altra chiusura nel terzo trimestre è stata avviata dagli stessi spammer, quando il programma partner SpaMIt, responsabile di enormi quantitativi di spam del settore farmeaceutico, ha annunciato la fine delle sue attività. I siti di questo programma, SpaMIt.biz e Spamit.com, hanno anche "postato" le motivazioni della loro chiusura concentrandole in "una lunga lista di eventi negativi nel corso dello scorso anno e la più intensa e maggiore attenzione prestata alle operazioni del nostro programma partner."

Il trend principale nel terzo quarto è stato l'allineamento tra l'industria dello spam e i produttori di virus. Lo spam oggi non è più un semplice fastidio, ma è una componente importante usata all'interno di schemi strategici illegali per rubare dati confidenziali, che possono essere usati per fare soldi. In ogni caso, questa situazione sta attirando l'attenzione dei legislatori e delle forze dell'ordine.



GUIDA

I SOFTWARE CONTENUTI NEL CD-ROM SONO SUDDIVISI IN 10 AREE TEMATICHE. ALCUNI DI ESSI SONO COLLEGATI AI TUTORIAL PUBBLICATI SULLA RIVISTA NELLE PAGINE CONTRASSEGNATE DAL LOGO "NEL CD".

HACKING

- FireSheep
- WinCap
- Sniff Pass
- Grinder
- IAS
- Spynet
- Mognet
- Essential NetTools
- WebCracker v4.0
- Udpflood

INTERNET

- Crazy Browser
- SlimBrowser
- SRWare Iron
- Firefox 4 beta 7
- Adobe Shockwave Player
- Xobni
- Nuri
- TorrentFetcher
- VDownloader
- YouTube Clip Extractor

PROGRAMMING

- jEdit
- EasyPHP
- Game Maker
- Xtreme Poll Generator
- Celerity
- Notepad++
- CSS Tab Designer
- FAQGenie
- DzSoft Perl Editor
- ASPhere

SECURITY

- Coyote
- Nessus
- SpywareBlaster
- Link Scanner
- Kruptos
- NoScript
- File Shredder 2
- Win Patrol 2010
- Sentry Lite
- Rising PC Doctor

AL CD

UTILITY

- FotoMix
- Image Converter One
- TSR Watermark Image Software
- M-Lat SMS Desktop
- IMCapture for Skype
- mIRC 7.15
- Miranda IM Portable
- Pidgin
- Visionica
- FaceBookCam

P2P

- Movie Torrent
- LimeWire Pirate Edition
- Bit Torrent
- Ares
- uTorrent
- LuckyWire
- Bearshare
- FrostWire
- eMule AdunanzA
- Mute

SYSTEM

- Ashampoo Magical Optimizer
- Wise Registry Cleaner Free
- Comodo System Cleaner
- Kludget Engine
- ReNamer
- HDClone Free Edition
- SyncBack
- GPU-Z
- Defraggler
- SiSoftware Sandra

NETWORKING

- MyLanViewer
- MyLanViewer Portable
- Teamviewer 6.0 beta
- OpenVPN
- UltraVNC
- VisualRoute Lite 2010
- NetWorx
- WeFi
- Connectify
- Gbridge

COPIARE

- BurnAware Free
- XMedia Recode
- Kool Media Converter 2.4.0.
- Cole2k Media Codec Pack Advanced
- Machete Video Editor Lite
- BurnAware Home
- Avidemux
- XviD Xvid
- DirectShow FilterPack
- Reezaa MP3 Converter

MULTIMEDIA

- Icecast
- Shoutcast
- Lame
- LiveIce
- Photomodeler
- ChrisTV Online! Free Edition
- Free Studio
- Grooveshark
- Xtreme Media Player
- Last.fm 1.5.4

INTERNET

NEL CD

COME COSTRUIRE UNA RADIO OPEN SOURCE

VOLETE CREARE UNA RADIO CHE TRASMETTE DALLA VOSTRA CAMERETTA SENZA SPENDERE UNA LIRA? ARMATEVI DEGLI STRUMENTI OPEN SOURCE NECESSARI E SEGUITE LA NOSTRA GUIDA.

di Massimiliano Rinaldi
redazione@hackerjournal.it

Ormai le radio trasmettono costantemente su Internet. Questo consente loro di superare le limitazioni costituite dalla portata limitata delle frequenze e di essere "udibili" in tutto il mondo.

Questa nuova prerogativa delle radio può essere sfruttata per cercare di allestire una radio "fai da te" con costi decisamente limitati, sfruttando solo software open source… Vediamo come.

Per realizzare uno studio radiofonico occorrono un server di trasmissione e un client per l'encoder (il codificatore) che possono anche stare su un unico server, sebbene sia preferibile separare i sistemi per ottenere il migliore risultato.

Oltre al nome di dominio è bene dotarsi di una connessione con IP statico, non che siano strettamente necessari, ma evitano di dover notificare di volta in volta agli ascoltatori l'IP dal quale trasmettiamo.

Nello schema di principio della stazione radiofonica digitale la voce proveniente dai microfoni in formato analogico viene inviata ad un mixer che concentra il flusso verso il client dove risiede l'encoder costituito dal programma Liveice; mentre LAME si occupa della conversione da analogico a digitale della voce e degli altri ingressi. Il server di trasmissione esegue Icecast, che utilizzando un formato di trasmissione del flusso ed una porta TCP/IP convenzionalmente riconosciuta dai comuni riproduttori MP3 ci permetterà di spedire su Internet la nostra programmazione radiofonica. L'aspetto più interessante è che processi differenti possono essere lanciati su server diversi configurati in maniera opportuna ottimizzando, ad esempio, la connessione di rete, le regole di filtraggio, il carico sulla CPU…) in modo che un servizio non inibisca l'altro.

Icecast è la controparte Linux (esiste anche una versione windows che trovate nel CD) del programma Shoutcast. Entrambi permettono di diffondere musica via Internet in tutto il mondo. E' come avere la possibilità di ascoltare la vostra stazione radio preferita dovunque voi siate. Il formato musicale abitualmente impiegato per le trasmissioni è MP3 con un rate dati di 32 o 64 kBps.

Questo rate così basso è necessario per garantire un buon flusso senza disturbi. I riproduttori MP3 memorizzano in un buffer di alcuni secondi i flussi da riprodurre provenienti da Internet, per sopperire ad eventuali piccole interruzioni.

Il formato MP3 permette di ascoltare la programmazione musicale a chiunque abbia Xmms o Winamp. Al momento il materiale in questo formato non richiede licenza, in ogni caso è meglio verificare sul sito http://www.mp3licensing.com/ se la società che detiene il brevetto impone i diritti. In alternativa ci si potrà spostare sul su uno schema di codifica/decodifica differente, come Ogg Vorbis, che non è sottoposto a brevetto e quindi non prevede il pagamento di diritti.

A prescindere, ed è importante viste le ultime evoluzioni legislative proprio in Italia, la trasmissione al pubblico di materiale tutelato con i diritti d'autore va svolta nel pieno rispetto delle normative. Assicuratevi di avere il permesso per trasmettere i brani di cui non siete gli autori materiali.

L'INSTALLAZIONE DEL SERVER

L'installazione di Icecast non è particolarmente difficile. Per prima cosa occorre scaricare da Internet il programma www.icecast.org. Scaricare la versione più recente e decomprimete il tutto:

```
tar zxvf icecast-1.x.x.tar.gz -C /tmp
cd /tmp/icecast-1.x.x/
```

Il programma va compilato digitando:

```
./configure
make
```

e come utente root installate il pacchetto:

```
make install
```

Questo comando copia tutti i file necessari al funzionamento su /usr/local/icecast. Il file di configuazione si trova in /usr/local/icecast/etc/icecast.conf. I settaggi più importanti sono:

```
# –first a few setting of the server and owner
#
#The location where the server is placed
location Music from the mars
#the owner's email address
rp_email webmaster@home.de
#The URL of the web page corresponding to the music
server_url http://www.linuxnetmag.de
[...]
#–You can administrate the icecast server via the network,
# this option is secured by a password
#normal clients should not be able to log in
client_password not_used
#The remaining passwords have to be changed
encoder_password mypassword
admin_password mypassword
oper_password mypassword
[...]
#The port icecast uses
port 8010
#The host name of the server
server_name my.computer.com
```

Lasciate stare gli altri parametri di configurazione, per il momento. Per lanciare il server per la prima volta, (come root sulla porta 8010), digitate:

```
/usr/local/icecast/bin/icecast -P 8010
```

Avrete qualcosa di simile al seguente output, se tutto è stato settato correttamente:

```
[09/Jan/2009:16:38:37] Icecast Version 1.3.0 Starting..
[09/Jan/2009:16:38:37] Using stdin as icecast operator
console
[09/Jan/2009:16:38:37] Tailing file to icecast operator console
[09/Jan/2009:16:38:37] Server started...
[09/Jan/2009:16:38:37] Listening on port 8010...
[09/Jan/2009:16:38:37] Using [linux.ulisse.local] as servername...
[09/Jan/2009:16:38:37] Max values: 20 clients, 10 clients per
source, 10 sources, 5 admins
-> [09/Jan/2009:16:38:37] [Bandwidth: 0.000000MB/s]
[Sources: 0]
[Clients: 0] [Admins: 1] [Uptime: 0 seconds]
->
```

Il sistema rimane in attesa di comandi, nel caso occorra configurare il server durante il suo funzionamento; digitando help, si ottiene una lista dei comandi disponibili in questo contesto.

Fino ad ora però, Icecast non invia musica perché non è ancora stato programmato per questo. Localizzate il file shout dentro /usr/local/icecast/bin/. Questo programma può essere avviato anche su un altro calcolatore sulla medesima rete; questo ha un senso perché dividendo il carico di lavoro tra il server che invia il flusso dati e quello che invece mantiene la lista di riproduzione si ripartisce meglio il carico di lavoro (ad esempio usando il secondo calcolatore, quello che funge da database MP3, anche per codificare in tempo reale in formato MP3 l'ingresso della scheda audio).

Pertanto, se lanciate shout sul medesimo server dove gira Icecast, il puntamento sarà a localhost, altrimenti occorrerà inserire l'indirizzo IP del server di riferimento. La porta sulla quale funziona Icecast di solito è la 8010, ma può ovviamente essere modificata secondo le esigenze.

Occorrerà poi stabilire una password utilizzata per il trasferimento dei file (parametrizzando admin_password in icecast.conf) e la directory dove sono residenti i file MP3.

Il comando che segue impartisce queste istruzioni tutte assieme:

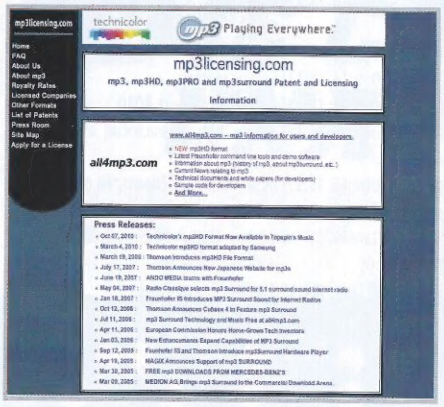
```
/usr/local/icecast/bin/shout localhost -P mypassword -e 8010
/tmp/mp3/*
```

Se tutto funziona a dovere adesso shout inizierà a trasmettere musica a Icecast:

```
Playing /tmp/mp3/Alice_in_Fashionland.mp3
[2:38] Size: 2219520 Bitrate: 112000 (28455 bytes/dot)
[.....
```

Mentre sulla consolle di Icecast vedremo l'esito della connessione:

```
-> [09/Jan/2009:17:37:57] Accepted encoder on mountpoint /
monkey from localhost.
2 sources connected
```




```
-> [09/Jan/2009:17:37:57] Assigning listeners from pending
source 3
-> [09/Jan/2009:17:37:57] Kicking source 3 [localhost] [Lost all
clients to new
source]
[encoder], connected for 10 minutes and 19 seconds, 824214
bytes transferred. 2
sources connected
-> [09/Jan/2009:17:37:57] Kicking all 0 clients for source 3
->
```

Adesso possiamo ascoltare la musica sulla porta 8010 alla quale puntano di default tutti i player MP3, ad esempio, usando freeamp:

```
freeamp http://my.server.local:8010
```

il programma si connetterà automaticamente a Icecast. Per avere una riproduzione di qualità migliore suggerisco di usare Xmms (mediante il quale è anche possibile creare la propria playlist, approfondite leggendo le istruzioni di configurazione di questo programmino).

Per gli utenti di Windows occorrerà creare un link nella propria home page dalla quale si vuole trasmettere la musica, in modo da lanciare automaticamente il player MP3, un esempio del codice HTML da inserire potrebbe essere questo:

```
<a href="shoutcast-playlist.pls"><img src="tunein.gif" Bor-
der=0></a>
```

posizionando il file shoutcast-playlist.pls nella stessa directory dove risiede la pagina dalla quale lo state richiamando. Il file shoutcast-playlist.pls ha la medesima sintassi, sia per Xmms che per i player Windows:

```
[playlist]
numberofentries=1
File1=http://my.server:8010
```

L'installazione di Liveice è senza sorprese. Tuttavia, prima di iniziare occorre installare un codificatore MP3. Raccomando l'uso di Lame perché lavora egregiamente assieme a Liveice. Questo programma è reperibile all'indirizzo: http://lame.sourceforge.net/. Dopo averlo scompattato digitando tar zxvf lame3.87beta.tar.gz -C /tmp occorre compilare ed installare il pacchetto:

```
cd /tmp/lame3.87/
./configure
make
make install
```

Seguite la medesima procedura per Liveice (che potete prelevare da: http://star.arm.ac.uk/~spm/software/liveice.html):

```
tar zxvf liveice.tar.gz -C /tmp
cd /tmp/liveice
./configure
make
make install
e copiate la directory (come root) in /usr/local
cp -a /tmp/liveice /usr/local
Liveice può essere configurato tramite un'apposita interfac-
cia, il file di configurazione si trova nella directory /usr/local/
liveice
cd /usr/local/liveice
./liveiceconfigure.tk
```

quindi impostate le seguenti opzioni:

-Server specifica il computer dove Icecast gira e al quale inviare l'audio. Nel caso sia il medesimo calcolatore dove fate lavorare il codificatore, scegliete localhost. Specificate anche la porta attraverso la quale il server ascolta il flusso dei dati;
-Impostate il formato PCM Audio a 32000Hz;
-Lo switch Soundcard deve essere selezionato. Se la vostra scheda audio supporta il full-duplex, cioè registra e manda in esecuzione contemporaneamente, attivate anche l'opzione omonima;
-Selezionate l'encoder, abbiamo detto LAME3 con un rateo di 32000 bit;
-poi impostate Soundcard only;
-nel campo Executables - Encoder inserite lame;
-Quindi salvate la configurazione nel file liveice.cfg ed uscite dal pannello di configurazione.
Come passo successivo occorre avviare Icecast, aprite una finestra terminale e digitate:

```
icecast
```

Dovreste visualizzare il seguente output:

```
Icecast Version 1.3.0 Starting...
Icecast comes with NO WARRANTY, to the extent permitted by
law.
You may redistribute copies of Icecast under the terms of the
GNU General Public License.
For more information about these matters, see the file named
COPYING.
[21/Oct/2009:00:47:33] Icecast Version 1.3.0 Starting..
[21/Oct/2009:00:47:33] Using stdin as icecast operator console
[21/Oct/2009:00:47:33] Tailing file to icecast operator console
[21/Oct/2009:00:47:33] Server started...
[21/Oct/2009:00:47:33] Listening on port 8010...
[21/Oct/2009:00:47:33] Using [muse.local] as servername...
[21/Oct/2009:00:47:33] Max values: 20 clients, 10 clients per
source, 10 sources, 5 admins
-> [21/Oct/2009:00:47:34] [Bandwidth: 0.000000MB/s] [Sources: 0]
[Clients: 0] [Admins: 1] [Uptime: 1 seconds]
->
```

Icecast è in attesa di ricevere il flusso dati. Per vedere l'elenco dei comandi, da console è sufficiente digitare ?, mentre per eseguirlo in background usate lo switch -b. In alternativa potete usare l'interfaccia web, richiamandola dall'url http://hostname:porta/admin/, dove hostname è il nome del vostro server (potete usare anche localhost) e porta il numero di porta definito nel file di configurazione icecast.conf. Assicuratevi di impostare una password, perché come impostazione predefinita, l'utility di amministrazione di Icecast basata sul web è aperta a qualsiasi sistema. Adesso lanciate Livelce:

```
./liveice
```

e dovreste visualizzare il seguente output:

```
playlist
0
Initialising Soundcard
16Bit 32000Hz Stereo
opening connection to 192.168.1.13 8010
Attempting to Contact Server
connection successful: forking process
opening pipe!...
writing password
Setting up Interface
Soundcard Reopened For Encoding
Input Format: 16Bit 32000Hz Stereo
Output Format: 32000 Bps Mpeg Audio
IceCast Server: 192.168.1.13:8010
```


```
Mountpoint: liveice
Name: Livelce Radio
Genre: Live
Url: http://www.miosituomusicale.local
Description: Livelce
Press '+' to Finish
Lvl: L: 5 R: 4
```

Il flusso dati viene spedito al server Icecast tramite Liveice:

```
-> [21/Oct/2009:00:51:58] Accepted encoder on mountpoint /icy_0
from linux.ulisse.local 1 sources connected
->
```

L'INPUT DI LINEA

Il mixer fornisce una vasta gamma di opzioni per l'input. Durante la trasmissione si possono scegliere quindi le sorgenti più diverse o i file MP3 già memorizzati sul disco fisso. Liveice richiede una qualità particolare per l'ingresso audio, se il volume di registrazione è troppo basso, non si sentirà nessun segnale in uscita, viceversa, se è troppo alto saturerà l'ingresso del mixer. Come nelle stazioni tradizionali, basterà ascoltarsi e regolare i valori per il risultato migliore. Come mixer software potete provare kmix, gmix o xqmixer. Adesso la vostra stazione radiofonica è pronta.

TRASMISSIONE AUDIO/VIDEO

Un possibile impiego alternativo potrebbe essere quello di inviare l'audio in abbinamento ad una sorgente video. Esistono numerosi documenti sulla rete e articoli apparsi sulle riviste specializzate che spiegano come predisporre un server per lo streaming video. Ovviamente è possibile fruire i programmi ricevuti dalla scheda TV da qualsiasi parte ci si connetta, ma lo svantaggio deriva dall'impossibilità di trasmettere anche la componente audio. Se diffondete le immagini di una web-cam, il suono non è molto importante, ma cos'è una trasmissione televisiva senza audio?
Dando per scontata quindi questa configurazione di base, potrete trasmettere in contemporanea l'audio scegliendo il bottone Rec. sotto la parte di mixer che riguarda la sorgente (CD, Line-In oppure microphone) che desiderate gestire. Dal lato dell'ascoltatore occorre oltre al browser un qualsiasi riproduttore MP3 che sia interfacciabile ad Icecast (per esempio xmms, freeamp, mpg123).

```
mpg123 http://my.server.local:8010
```

E' molto importante specificare la porta di lavoro corretta. Adesso potrete ricevere il video proveniente dalla scheda TV ed il relativo audio ovunque voi siate semplicemente contattando il vostro server.
La codifica in tempo reale è più efficiente rispetto alla semplice riproduzione di un file MP3, che invece soffre il ritardo di riproduzione e quindi si avverte la mancanza di sincronia tra audio e video. Si può ovviare aumentando il numero di refresh ad almeno 20 per secondo, ma questo comporta un carico elevato di traffico sulla rete locale.
Qualcuno quindi ripiega facendo partire in ritardo il segnale video, in modo da sincronizzarlo con il momento della riproduzione MP3, sebbene in questo giochi ancora un ruolo il riproduttore MP3 dal lato client.

Riferimenti

-http://www.icecast.org/
-http://www.shoutcast.com (per ascoltare buona musica);

MULTIMEDIA
NEL CD

REVERSE E DIGITAL

di Massimiliano Rinaldi
redazione@hackerjurnal.it

Fotografare è un 'arte antica, forse digitalizzare con uno scanner una foto è un'arte un po' più recente ma, in entrambi i casi, possiamo dire di essere ormai abituati a fare entrambe queste due cose. L'evolvere della tecnologia, la diffusione sempre più massiccia di strumenti informatici, ci hanno portato a cercare o sperimentare nuove strade per comunicare, creare o ottenere ciò che vogliamo. Ai tempi del Commodore64 ci si stupiva per immagini sgranate in poche tonalità di grigio che impiegavano minuti per essere visualizzate e si sognava il giorno in cui sarebbe stato alla portata di tutti poter tenere un album fotografico digitale, oggi invece, con la grafica poligonale dei moderni videogiochi 3D, ci viene spontaneo chiederci quando sarà possibile per ognuno di noi poter creare oggetti manipolabili interattivamente senza essere dei designers 3D ed avere apparecchiature costosissime. Già, perché proprio di questo si tratta, di accessibilità da parte di tutti a questa nuova arte. In particolare in questo articolo tratteremo come trasformare oggetti realmente esistenti in oggetti tridimensionali digitali pur senza usare programmi professionali di modellazione tridimensionale o CAD e senza dover avere assolutamente a che fare con termini tipo nurbs, solidi particellari ecc..

INGEGNERIZZAZIONE INVERSA

Molto spesso quando si pensa a modelli in computergrafica si pensa al geometra che è costretto a progettarsi una casa con il CAD partendo da zero o ad un designer che prima di ricreare un oggetto deve prima cercarsi decine di texture diverse da applicare alle superfici del modello. In realtà la progettazione di sintesi cioè la creazione di un modello ex novo partendo da zero, linea per linea, poligono per poligono, scegliendo la texture per ogni superficie è divenuta una metodologia di nicchia, relegata soprattutto al mondo aziendale ed in particolare con riferimento alla tecnologia. Nella maggior parte degli altri casi invece, soprattutto nell'industria dell'entertainment, cinema, video musicali, videogiochi, spot televisivi o illustrazioni, il metodo più rapido e più diffuso per creare modelli realistici di oggetti è quello dell'ingegnerizzazione inversa e cioè si parte dal modello reale o più spesso da una sua riproduzione in scala e lo si digitalizza. Per digitalizzare l'oggetto in questione esistono metodi professionali molto costosi, come bracci misuratori che segnano svariati punti sulla superficie dell'oggetto trasferendoli nell'identica posizione nel PC, oppure, costose scansioni laser che disegnano sull'oggetto una griglia la cui trama deve essere tanto più fitta quanto più precisa si vuole che sia la digitalizzazione dello stesso. In questa nostra discussione però siamo interessati a metodi più accessibili usando programmi commerciali facilmente reperibili (o quasi… come avrete modo di scoprire). Questi programmi utilizzano tutti una o più normali fotografie 2D provenienti da acquisizioni con un normale scanner o catturate con la propria fotocamera, si differenziano però in un diverso approccio tecnico per estrarre la terza dimensione: alcuni usano dei solidi 3D predefiniti da

ENGINEERING 3D

COME EFFETTUARE LA SCANSIONE DI UN OGGETTO TRIDIMENSIONALE

sovrapporre a strutture simili presenti nell'immagine scegliendo solo il corretto orientamento e la giusta dimensione, altri invece sfruttano la sagoma dell'oggetto ripreso da più direzioni per stabilirne la forma, tecnica più raffinata ma che richiede una maggiore quantità di immagini.

RICOSTRUZIONE CON SOLIDI PRESTABILITI

All'inizio fu Canoma: Alcuni anni fa una azienda che allora si stava facendo conoscere, la Metacreations, mise sul mercato quasi in punta di piedi un programma strano che serviva a trasformare foto 2D in oggetti 3D, o meglio, estrarre oggetti tridimensionali da foto bidimensionali e questi potevano essere semplici scatole appoggiate su un tavolo sia grandi edifici cittadini immortalati su una cartolina per turisti. L'interfaccia utente che dir semplicissima è dir poco ha subito conquistato una larga fetta di pubblico non esperto e la disarmante bellezza dei risultati unita ad un'incredibile velocità per ottenerli hanno contribuito ad aumentarne la fama anche tra i professionisti. Canoma permetteva, grazie ad un set di forme geometriche prestabilite di ricostruire oggetti da fotografie 2D. Il funzionamento era semplicissimo, bastava caricare inizialmente una sola immagine e sovrapporre ad essa dei solidi geometrici prestabiliti visualizzati in modalità "filo di ferro" in modo da farli combaciare con vertici e spigoli degli oggetti visibili nella foto. Movendo opportunamente i vertici dei modelli, il programma riusciva a calcolare autonomamente alcune caratteristiche spaziali dell'immagine quali la focale e l'angolo visuale, applicando così la giusta distorsione ai solidi per farli

Canoma bastano due solidi per definire la forma di una capanna.

combaciare. Una volta posizionati tutti i solidi, ad esempio per la foto di una capanna bastavano un parallelepipedo a sezione rettangolare alla base ed uno a sezione triangolare come tetto, si premeva il bottone di rendering ed il programma applicava su ogni superficie dei solidi la parte di foto corrispondente come texture. La pecca più grande di questo programma oltre a qualche bug di troppo è sempre stata la mancanza di solidi di rotazione come sfere, semisfere, toroidi (ciambelle) o cilindri, rendendo così assai arduo o praticamente impossibile ricreare bicchieri, palloni o cupole di edifici. Purtroppo, con il fallimento dell'azienda Metacreations, Canoma venne svenduto alla Adobe che dopo aver promesso di realizzarne una nuova versione con solidi di rotazione, preferì insabbiare il programma. Attualmente Canoma è quasi introvabile a patto che non abbiate da parte qualche raccolta CD di 5-6 d'anni fa.

Photomodeler: Parallelamente allo sviluppo e morte di Canoma, venne alla luce un altro programma con doti simili: Photomodeler (http://www.photomodeler.com). Già da un primo sguardo però si notava un'impostazione diretta decisamente ad un pubblico professionale, un'interfaccia decisamente poco user-friendly, perlomeno all'inizio, e una certa tendenza alla precisione più che all'estetica. Photomodeler infatti si presenta tuttora come un programma di fotogrammetria con doti di ricostruzione 3D, quasi un CAD ma, anziché costruire le immagini dal nulla, le ricostruisce partendo da misurazioni accurate di fotografie 2D. I suoi creatori infatti lo consigliano per la ricostruzione a fini legali della dinamica di incidenti, ad esempio misurando la lunghezza di una frenata sull'asfalto immortalata in una foto dai carabinieri. Dato che è così orientato alla fotogrammetria ed è decisamente di utilizzo impegnativo, risulta poco pratico per la ricostruzione di oggetti o ambienti a fini estetici ma rimane comunque uno dei migliori programmi di ricostruzione 3D partendo da foto 2D. Il suo costo è attorno ai 995 dollari..

Canoma, aggiungendo altri solidi si aumentano i dettagli della ricostruzione.

Canoma, una volta ricostruito il modello è possibile ruotare la scena e vederla da più angolazioni come non era possibile fare nella fotografia 2D.

Geometra 3D: Sullo stesso stile di Photomodeler ma nato molto prima, forse addirittura in concomitanza con Canoma, Geometra 3D si presentava come un programma dall'interfaccia utente un po' scarna tanto da non lasciar intendere tutta la potenza e versatilità di cui invece poteva farsi vanto. Con una toolbar di soli sei pulsanti permetteva di caricare tutte le foto necessarie, meglio se più di due e da direzioni diverse, calibrare le immagini e renderizzare il modello. A differenza di Canoma che calibrava la focale delle immagini analizzando le deformazioni che l'utente applicava ai solidi, Geometra 3D preferiva una calibratura ad opera di marcatori, cioè di punti speciali delle immagini che l'utilizzatore doveva marcare su ogni foto stando bene attento a dare loro lo stesso numero d'identificazione. Successivamente si poteva passare alla ricostruzione del modello vero e proprio anche qui con un metodo completamente diverso da quello usato da Canoma, qui infatti non esistevano forme e solidi predefiniti e tutti gli oggetti dovevano essere ricostruiti unendo i vertici uno ad uno con linee e dicendo al programma di volta in volta quali dei poligoni risultanti dovevano essere trasformati in superficie da texturizzare, inoltre si poteva anche scegliere quale delle foto doveva essere usata per texturizzare quel poligono. Tutte queste caratteristiche rendevano il programma impegnativo e lungo nella produzione di modelli ma in compenso permetteva di ottenere risultati anche migliori di quelli ottenibili con Canoma e soprattutto permetteva di ricostruire anche oggetti dalle forme complesse, curve e non regolari come un viso umano o delle rocce. Avrete notato che parlo al passato anche per questo programma, anch'esso infatti come Canoma è sparito nell'oblio e si è fermato alla versione 1.1. Un vero peccato perché c'erano larghi margini di miglioramento che avrebbero potuto farlo diventare famoso.

Autodesk image modeler: Più recente nonché uno dei pochi in vita assieme a Photomodeler, il francese Image Modeler (ex Realviz), acquisito di recente da Autodesk, è decisamente il più potente di tutti e consapevole di ciò è anche molto costoso per le tasche di un utente domestico: 995 euro L'interfaccia ben curata ordina in modo razionale dei menù con tools e bottoni numerati guidano l'utente nel percorso sempre più impegnativo nell'estrazione dell'oggetto 3D dalle fotografie inserite. Il bottone 1 riguarda la sezione iniziale di creazione del progetto in cui si caricano le immagini da utilizzare.

Nella sezione 2 si comincia con la prima parte, quella forse più impegnativa e che spesso fa imbestialire, la calibrazione delle immagini. Il metodo per scoprire la focale e la posizione delle camere nel riprendere l'oggetto che viene usato da Image Modeler è inizialmente simile a quello usato da Geometra 3D cioè marcatori da posizionare a mano in ogni fotografia ognuno sul medesimo punto dell'oggetto ripreso da varie angolazioni. Dopo che si è raggiunto un totale di circa una decina di marcatori collocati su ogni foto si nota però una differenza fondamentale da geometra 3D che dimostra tutta la potenza di Image Modeler, cioè il posizionamento automatico di tutti gli altri marcatori. In altre parole i primi marcatori vengono messi a mano su tutte le immagini dall'utente per permettere al programma di farsi un'idea delle focali e delle direzioni di ripresa, poi non appena i calcoli lo permettono, basta inserire un marcatore sulla prima immagine che il programma lo triangola nelle tre dimensioni su tutte le altre foto con un cerchietto attorno che rappresenta lo scarto d'errore. All'utente non resta che aggiustare i marcatori che hanno il cerchio più grosso ed ecco che la calibratura migliora ulteriormente. Questo lavoro, soprattutto nella prima parte per il posizionamento manuale della prima decina di marcatori può essere particolarmente lun-

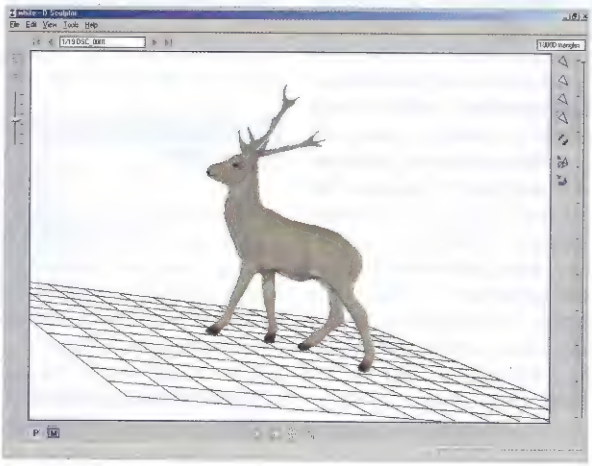
go e snervante ma le features di zooming automatico e di antialiasing permettono di ottimizzare al massimo il lavoro.
Calibrate le camere si passa alla sezione 3 dove comincia la definizione dell'oggetto vero e proprio, con la costruzione del modello. Partendo dai marcatori di calibrazione o da altri aggiunti successivamente sui vertici delle figure si può iniziare a costruire il proprio modello ma anche qui il programma dimostra tutta la sua potenza mettendo a disposizione sia la costruzione in stile Geometra 3D cioè linea per linea poligono per poligono, sia quella in stile Canoma con solidi predefiniti da far combaciare alle immagini. Soprattutto questa seconda possibilità dimostra una certa versatilità prima di tutto nel fatto di avere a disposizione solidi di rotazione come sfere e cilindri ma poi anche nel fatto di avere anche modelli di oggetti comuni come dischi da trasformare in piatti o scodelle o una maschera da applicare ai visi umani, inoltre è persino possibile importare modelli personalizzati da altri programmi.
Una volta ricreato il modello sulle immagini si passa alla sezione 4 che contiene i tools per scegliere quali superfici vanno texturizzate poi si passa alla sezione 5 che permette di esportare il modello.
Image Modeler è in assoluto il più potente e versatile tra i programmi di questo genere anche perché oltre a lui ormai esiste solo Photomodeler... ma sarebbe auspicabile venisse fatto qualche intervento di semplificazione soprattutto per renderlo più semplice nella sezione 3 per la costruzione dei modelli in cui le tante opzioni disponibili lo rendono poco comprensibile, inoltre non sarebbe un brutta idea se creassero una versione "leggera" semplice come Canoma e magari gratuita per scopi non commerciali così da accontentare anche il pubblico dei non professionisti.

Ricostruzione da scansione della sagoma dell'oggetto reale: Questo tipo di ricostruzione è molto simile a quella effettuata dalle T.A.C. ospedaliere che creano un modello partendo dalla sagoma in sezione. Lo stesso fanno questi programmi che permettono così di definire oggetti anche molto complessi o privi di forme geometriche regolari. L'unico lato negativo però è che per ottenere buoni risultati sono necessarie molte fotografie.

Real2virtual modeller: Con questo programma ci addentriamo nel metodo più strano e recente usato per la ricostruzione di oggetti in 3D, non si tratta di un programma molto complesso ma, una volta superata la parte iniziale un po' caotica, si possono ottenere risultati molto interessanti. Come al solito, la prima cosa da fare quando si digitalizza un modello è specificare le direzioni da cui è stato ripreso l'oggetto originale. Due metodi sono disponibili: fornire direttamente i dati precisi, oppure, lasciare che Real2virtual Modeller calcoli i dati per voi. Nel primo caso dovete dire voi al programma focale, distanza e angolo di ripresa delle foto specificando se la foto rappresenta il davanti, il dietro o un lato dell'oggetto con la possibilità di inserire i gradi precisi. Nel secondo caso dovete fare un piccolo wizard di configurazione in cui vi si chiede di dare delle informazioni sul tipo di fotocamera usata potendo anche scegliere la vostra tra un set di fotocamere di marche conosciute, dopodiché sarà il programma a calcolare la direzione e la focale di ogni immagine. In quest'ultimo metodo però è necessario un piccolo accorgimento che diventa limitativo solo in caso si voglia riprendere di grandi oggetti e cioè è necessario che l'oggetto poggi su una base rettangolare, ad esempio un foglio di carta, sul quale dovrete marcare degli angoli per aiutare il software nei suoi calcoli.
Una volta calibrate così tutte le inquadrature, potrete passare alla definizione della silhouette del modello da digitalizzare. Con dei tool simili a quelli di qualunque programma di fotoritocco non dovete far altro che impiegare qualche ora del vostro tempo a rifinire la sagoma dell'oggetto in ogni foto. Una volta finito premete il bottone di costruzione del modello e, grazie all'intersezione di migliaia di rette immaginarie, ecco che si formerà la versione digitale del vostro oggetto con tanto di texture.

D-sculptor: Forse si tratta del primo programma di questo tipo mai creato prima, anche per questo ha un costo notevole. Basta riporre sotto l'oggetto da fotografare un semplice foglio con un motivo geometrico stampato sopra ed ecco che il programma calcola automaticamente focale, distanza, inclinazione e angolo, senza chiedere nessuna informazione sulla camera usata. L'interfaccia semplicissima lo rende utilizzabile da chiunque e la semplicità unita al realismo ottenibile fanno venire in mente Canoma. Con una quindicina di fotografie ben nitide è possibile ricreare qualunque oggetto e l'unica cosa che richiede un minimo di pazienza è la definizione della sagoma. A suo seguito sono nati altri programmi simili come 3D snapper ed UZR 3D che però non aggiungono nulla di nuovo.

D-sculptor l'oggetto da digitalizzare posizionato sopra la base con foglio prestampato.



D-sculptor il modello ricreato e texturizzato.

E-MAIL

TENTATIVI DI PHISHING CI ARRIVANO OGNI GIORNO E CON TECNICHE SEMPRE PIÙ SOFISTICATE. IMPARIAMO A SMASCHERARLI APPRENDENDO I TRUCCHI USATI DA CHI LE CREA, IN MODO DA DIFENDERCI. PREVENIRE È MEGLIO CHE CURARE...

di G.ENOMA
redazione@hackerjurnal.it

L'obiettivo è semplice: andare a pesca di sprovveduti che forniscano, a chi invia la mail, dati sensibili quali credenziali di accesso a siti finanziari, social network o siti di gaming. Il meccanismo funziona così: riceviamo una mail che ci comunica un evento (che può essere piacevole o spiacevole) e ci invita ad agire. I toni possono essere gioiosi (hai vinto!) o minatori (se non agisci subito sono guai). Con rare eccezioni, l'azione è sempre la stessa: fare click su un link presente nella mail. A quel punto ci si trova in una pagina del tutto simile a quella del servizio vero, ma peccato che è fasulla, dove ci è richiesto di fornire delle informazioni (come ad esempio fare il login). E a quel punto la trappola ha avuto effetto: i nostri preziosi dati sono inviati al truffatore di turno. Nei casi più sofisticati, veniamo poi anche rediretti sul sito vero dopo un messaggio tipo "riprova, login errato" (chi non sbaglia mai almeno una volta ogni tanto?).

COSA VOGLIAMO IMPARARE?

L'obiettivo dell'articolo è di fornirci gli strumenti per capire se una email è veritiera o se magari, sotto quella parvenza di autenticità si nasconde invece un tentativo di raggirarci. Parliamo di strumenti, ma non di programmi software che ci diano una risposta pronta. Strumenti intesi come acquisizione di quelle conoscenze che ci permettano di analizzare criticamente i contenuti delle email. E siccome quel chilo e mezzo di materia grigia che ci portiamo appresso è il miglior computer del mondo, questi saranno di fatto i migliori "tools" di cui potremmo dotarci.
Acquisiremo questo bagaglio di esperienza analizzando esempi concreti di phishing e sviscerandone le problematiche, sia quelle più ovvie (che già ci permettono di smascherare una buona percentuale di casi), che quelle meno appariscenti, e in quanto tali più subdole.

UN CLASSICO: VINCITA CON LA CARTA DI CREDITO

Partiamo subito con la figura 1, un classico. L'ente della carta di credito ci scrive. La strategia è quella di non metterci sulla difensiva. Non c'è nessuna intimidazione, ma una notizia positiva: abbiamo vinto qualcosa (a chi non farebbe piacere?). È

PHISHING

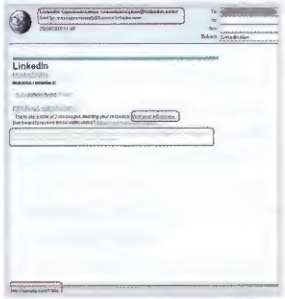
Tipico phishing che simula una mail di CartaSi, con link fasulli e aspetti psicologici per farci abbassare la guardia

noto che questo fa abbassare le difese critiche nella maggior parte delle persone, e ciò è fondamentale per cadere nella trappola, che altrimenti risulterebbe ovvia. Innanzitutto chiediamoci se abbiamo una carta di quel circuito: sembra ovvio, ma una significativa percentuale di coloro che ci cadono non fa caso alla cosa. Se non la abbiamo, buttiamo la mail con serenità.

Partiamo dall'alto: il mittente sembra legittimo: il dominio è "cartasi.it" come quello vero. Anche il link mostrato nella pagina mostra un URL consistente (www.cartasi.it). Tuttavia, posizionando il cursore del mouse sopra questo URL (ATTENZIONE: senza fare click!) potremo osservare nella barra di stato del nostro programma di posta quale sarà il vero URL a cui andremo se facciamo click. Se guardate nel riquadro in basso, potrete notare che punta a "www.gubego.net": niente a che fare con "cartasi.it". Ecco scoperto il tentativo. Da questo abbiamo imparato che il testo di un URL cliccabile non necessariamente corrisponde al vero URL a cui verremo portati seguendone il collegamento. Ma ci sono altri indicatori che in questa mail c'è qualcosa che non va. Innanzitutto: abbiamo partecipato veramente al concorso? Forse potremmo non ricordarci, ma già questo ci deve mettere sull'avviso (e poi spesso questi concorsi non durano un solo mese). Guardiamo poi bene il testo riquadrato in verde. Leggendolo con attenzione (cosa che quasi nessuno fa), ci accorgeremo di vari errori di grammatica: "informarvi" "informarla"; "questo premio mese" "questo mese il premio". Le aziende bancarie hanno dipartimenti specializzati per la formulazione di comunicazioni agli utenti, e non fanno simili errori. Tuttavia statisticamente solo una piccolissima percentuale di persone si accorge o da peso all'errore, che invece è un indicatore importantissimo: spesso infatti le mail di phishing sono originate all'estero da persone che usano traduttori automatici. Una sottigliezza finale per coloro con una infarinatura di programmazione: l'URL visualizzato mostra la stringa "id=vincitore". Nei casi reali, come meccanismo sia di sicurezza che per funzioni di puro tracking nei nostri comportamenti, ci saremmo aspettati una stringa tipo "id=<<codice_univoco_che_ci_identifichi>". In tal modo potranno collegare la mail inviata alle nostre azioni sul sito.

L'ALERT DAL SOCIAL NETWORK

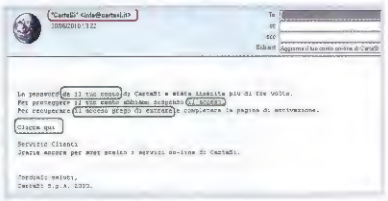
Saltiamo ad un altro argomento: le notifiche da un social network. Con riferimento alla figura 2, parliamo di Linked-In. Ritroviamo molti degli elementi visti nel caso precedente: appartenenza effettiva al network e gli elementi riquadrati in rosso per URL che non corrispondono. In questo caso però il testo del link non è un URL esplicito e questo è parte di un altro tipo di strategia psicologica. Se infatti la presenza di un URL stimola automaticamente il desiderio di verifica (anticipata, quello che abbiamo fatto in precedenza, o posticipata, ovvero guardare la barra degli URL nel browser), un normale testo cliccabile tende a non attivare questo meccanismo di analisi. Sottigliezze che però fanno cadere nella trappola molti incauti. Una nota di umorismo: leggete il messaggio in verde sulla tutela dei dati personali. In realtà succederà esattamente il contrario: non solo verranno catturati i vostri dati di accesso, ma il truffatore di turno potrà anche confermare che la vostra e-mail è valida, e venderla al fiorente mercato degli spam. Ultima annotazione: Ashlee Xiong dice di essere una vostra amica. Se non la conoscete sapete cosa dovete fare: il cestino è lì che aspetta.



Phishing che simula una mail di un social network come LinkedIN.

PROBLEMI DI ACCESSO AL SITO DELLA CARTA DI CREDITO

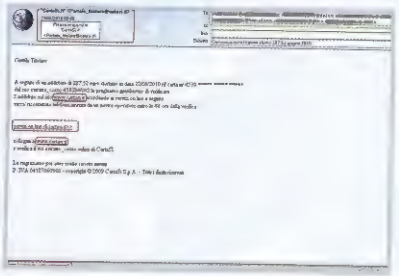
Passiamo alla figura 3. Sembra una mail più innocua delle precedenti. Differentemente dai casi appena visti infatti non presenta alcun link cliccabile. Tuttavia essa implementa altri due cardini del phishing, molto efficaci. Essa crea una situazione di allarme, con il nostro conto bloccato per motivi di sicurezza. Questo stimola la necessità di risolvere con urgenza. La mail non presenta, ad arte, alcun punto di contatto (niente URL, niente telefono). L'unica cosa visibile è l'indirizzo di mail del mittente, che sembra legittimo. Quello che in pratica accade è che la persona, presa dal panico, risponde (reply) alla mail dicendo cose tipo: ho ricevuto questa mail. Il mio account e pwd sono queste: mi potete comunicare le nuove? Molto più facile ed efficace che non creare un sito web di phishing. Notate la quantità di errori di grammatica (riquadrati in verde): rimarrete sbalorditi dal fatto che in pochi li notano e/o considerano importanti. In particolare l'errore grossolano di questa specifica mail è che hanno lasciato il testo "Clicca qui", senza che ad esso corrisponda un link.



Altro esempio che simula una mail di CartaSi, minatorio e senza link, ma quanti errori!

UN ALTRO CASO DI FRODE CON CARTA DI CREDITO

Passiamo alla figura 4. Qui ritroviamo, riquadrate in rosso, tutte le problematiche collegate con gli URL falsificati, ma con una interessante variante: i due link www.cartasi.it puntano effettivamente al sito ufficiale, mentre quello "servizi on line di cartasi" invece punta al sito di phishing (parzialmente camuffato dal nome "cartasigtw" all'inizio. Quindi attenzione: il fatto che un link sia corretto, non significa che lo siano tutti.



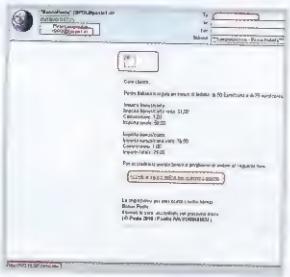
Qui vediamo all'opera altre tecniche, ma quanti destinatari...

In realtà questa mail ci avrebbe dovuto insospettire per un altro aspetto. Se guardiamo il titolo, si riferisce allo storno di una operazione con un certo valore definito al centesimo. Ma allora perché come destinatari della mail ci sono così tante persone (per privacy ho camuffato i nomi)? La statistica ci dice che sarebbe anche possibile (con una probabilità inferiore a quella di vincere al Superenalotto) che in tanti abbiano diritto ad uno storno della stessa cifra per una operazione effettuata lo stesso mese e con lo stesso circuito di carta di credito. Ma il punto è che motivi di privacy sarebbe comunque stata mandata a ciascuno una comunicazione separata.

Altre due segnalazioni. Intanto il mittente "Portale_Titolare@": non è proprio una dicitura in Italiano. Ci saremmo al limite attesi "Portale_Titolari@". E poi, se guardate bene, il dominio di posta del mittente è "@catasi.it" e non "@cartasi.it". Alzi la mano chi se ne era accorto. Questo ci apre la porta ad un'altra considerazione collegata al funzionamento del nostro cervello che ci può fare brutti scherzi e non permetterci di vedere l'ovvio. Si è dimostrato che mentre leggiamo un testo il cervello non legge realmente tutte le lettere, ma appena crede di aver intuito una parola, passa alla successiva. Questo è il motivo per cui il lavoro di correttore di bozze è così impegnativo. Ed è anche il motivo per cui ciascuno di noi ha realmente letto "cartasi.it" anche se non era scritto così. Una ragione in più per cui molti non si accorgono degli errori di queste mail, e abboccano.

NON POTEVA MANCARE BANCOPOSTA

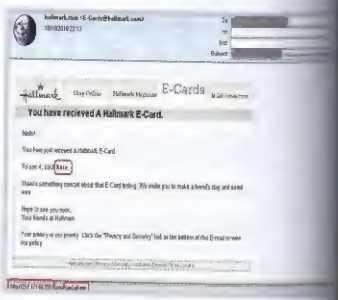
Figura 5 mostra una serie tutta diversa di problematiche. Un classico caso di camuffamento. Partiamo dal mittente: il dominio "poste1.it" è una variante che sembra essere legittima, ma in realtà sappiamo che chiunque può registrare il dominio "poste1.it". Inoltre, se guardiamo il vero URL del link cliccabile, stranamente punta a un indirizzo IP diretto e non usa il FQDN (Fully Qualkified Domain Name, ovvero qualcosa tipo www.poste1.it come ci aspetteremmo). Ci si può divertire con la utilità di sistema nslookup presente su tutti i sistemi (lo lascio come esercizio...), ma in realtà solo in pochissimi si prenderebbero una simile briga, accettando che quell'IP sia anche esso ragionevolmente legittimo. Sappiate che nessuna banca farebbe mai una cosa simile, perché si esporrebbe ad una serie di rischi in caso di frode accertata, primo tra tutti quello di concorso di colpa (l'utente non avrebbe strumenti efficaci per verificare). Ma notiamo un'altra cosa: la mail ci è arrivata, ma nel campo destinatario non c'è nessuno. Questo comportamento (ovvero mettere i destinatari nel campo bcc: (Blind Courtesy Copy - copia nascosta di cortesia) è tipico dello SPAM, e il phishing non è che una variante aggressiva di questo sistema, che prevede l'invio di mail identiche a di centinaia di migliaia di persone. Un'ultima chicca: "BancaPosta" o "BancoPosta"? Sono i dettagli che fanno la differenza...



Esempio con altre tecniche di camuffamento del FQDN, ma dov'è i destinatario?

CARTOLINE CHE PASSIONE

Tempo fa andavano più di moda, ma ancora oggi hanno il loro seguito: spedire a qualcuno una cartolina elettronica con un'animazione, una bella poesia e/o musica era un bel modo di mandare un messaggio meno asettico di una mail o di un SMS. L'esempio in figura 6 ci mostra una ulteriore tecnica. I link non ci portano ad un sito simulato dove catturare le nostre credenziali, ma ci fanno eseguire un programma ("cardgif.exe"). Considerando che (ahinoi) negli ultimi anni a poche persone hanno spiegato che ciascun file ha una estensione e che l'estensione ha un significato (tutti i sistemi operativi cercano di nascondere questo supposto tecnicismo), in molti non faranno caso al suffisso ".exe" e si soffermeranno sul "cardgif", immaginando di aprire una immagine grafica. E allora il phishing agisce in due passi: installa tipicamente un keylogger che si occuperà poi di catturare informazioni sensibili e trasmetterle a chissà chi a nostra insaputa. Notate che questo tipo di phishing in due passi è particolarmente insidioso in quanto, non trattandosi di fornire dati bancari, le nostre "difese immunitarie" si abbassano molto.



Esempio di e-card: strategia di phishing in due stadi.

REPETITA JUVANT...

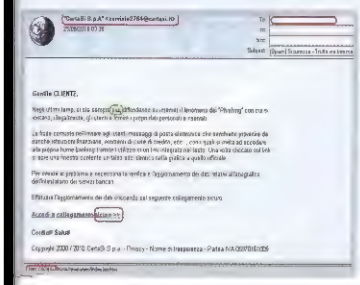
...dicevano i romani. Ovvero: meglio ripetere, se è importante. Ma è sempre vero? Figura 7 mostra un caso in cui apparentemente la nostra banca ci tiene talmente a noi da inviarci lo stesso messaggio due volte nella stessa giornata. In un caso il messaggio è identico, nell'altro c'è un sospetto "[Bulk]" (che tra l'altro non è una parola italiana e non verrebbe mai usata da una banca). Sappiate che tali ripetizioni non esistono, e sono un forte segnale di spedizioni massive ("bulk") di messaggi di phishing.

	Poste Italiane	18/10/2010 21.47	4.313	Posteitaliane * Nuove misure di sicurezza 2010 *
	Poste Italiane	18/10/2010 20.23	4.800	[Bulk] Posteitaliane * Nuove misure di sicurezza 2010 *
	Poste Italiane	15/10/2010 18.11	3.461	Poste Italiane ti regala un bonus di fedelta !
	Poste Italiane	15/10/2010 15.06	3.404	Poste Italiane ti regala un bonus di fedelta !

Esempio di invio ripetuto della stessa mail, sintomo che qualcosa non va.

MASCHERAMENTO ATTO SECONDO

Guardiamo ora il caso di figura 8. Lo segnalo perché a fianco ad alcune problematiche già viste (mittente invisibile e link a sito certamente fasullo), ci sono altre due cose molto importanti, che potrebbero sfuggire ad una prima occhiata. La prima è una tecnica di camuffamento che è molto efficace, ma che qui è stata applicata solo in parte.
Se guardate il mittente noterete che il dominio è "@cartasi.lt". Non vi dice nulla? Se lo scrivo in maiuscolo il problema appare chiaro: "@CARTASI.LT" e non "@



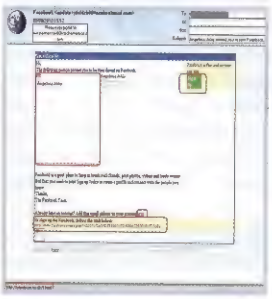
Altri tipi di errori e tecniche di camuffamento a cui fare attenzione. In particolare guardate il dominio mittente: "LT" non è lo steso di "IT", anche se in minuscolo si assomigliano.

CARTASI.IT". Se il link cliccabile avesse puntato anche a "www.cartasi.lt", sarebbe stato veramente difficile accorgersi del problema. I FQDN non sono "case sensitive", ovvero maiuscole e minuscole non fanno differenza e si può giocare su questo per imbrogliare il cervello: chi distingue una l (i) maiuscola da una I (L) minuscola con questo font? Ma c'è una altro aspetto da notare: chi ha scritto questa mail usa probabilmente un computer con un set di caratteri non uguale al nostro. A parte il "toulari" nell'URL vero, se guardate la parola riquadrata in verde dimostra che le lettere accentate non sono correttamente riprodotte. Ironicamente questa mail (vale la pena leggerla tutta) dà una descrizione particolarmente corretta di ciò che il phishing fa, e ciò che loro stanno per farci.

Avendola letta tutta, vi sarete probabilmente accordi dell'ultimo punto degno di nota. Si evidenzia il fatto che il collegamento è "sicuro", ma in realtà l'URL puntato mostra il classico "http://" e non "https://" come ci aspetteremmo.
Tutti piccoli indizi che ci aiutano a capire come stanno le cose.

FACEBOOK...

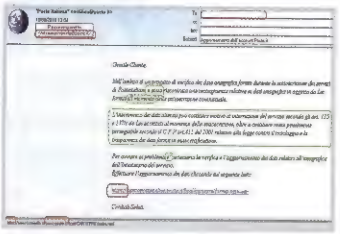
Non poteva mancare uno dei siti "social" più gettonati (figura 9). L'elemento più evidente è la non consistenza tra il link mostrato per esteso e quello reale ("capelcure.co.uk"). Non ha alcun senso. Inoltre tutti i link puntano a questo stesso URL anche se dovrebbero portarci a sezioni diverse. Tuttavia questo tipo di mail ha un grande successo (per chi la invia) a causa del fattore psicologico sottostante: solletica la nostra curiosità e il nostro ego vanesio. Per i maschietti, Angelina Jolie ha invitato proprio noi (e ne esiste una versione per le femminucce). Siamo seri: a meno che non la conosciate di persona o che voi non siate persone famose, realmente un personaggio noto vi contatterebbe direttamente? Ci sono altre cose da notare in questo phishing (suggerimento: i due indirizzi del mittente e il sito di arrivo), ma li lascio a voi.



Una mail di un social network come Facebook. Qui la tecnica è più psicologica che tecnologica.

BANCO POSTA ATTO SECONDO

Figura 10 ci porta all'ultimo caso presentato in questo articolo. Innanzitutto le singole parole riquadrate in verde, che indicano numerosi ma piccoli errori, compresa la non disponibilità di lettere accentate (importante), che non sono facili da notare. Il tono qui è decisamente minatorio e il linguaggio tipico del "legalese". Contiene riferimenti normativi che nessuno andrebbe mai a verificare (anche se si può fare con semplicità andando a riprendere il contratto). Il problema è comunque che in molti di questi casi i riferimenti normativi potrebbero anche essere corretti. Possiamo riconoscere anche altre problematiche che già ci danno una indicazione chiara. Ma le novità di questa mail sono altre. Intanto il link a cui fare click menziona esplicitamente "https", a garanzia (teorica) di sicurezza. In realtà il link vero è un "http" semplice, e questo è un segnale fondamentale. E sopratutto poniamo attenzione ad una nuova tecnica di camuffamento, sempre volta ad ingannare il nostro cervello. Se guardate il link vero, noterete che l'URL contiene la stringa "www.poste.it". Peccato che sia solo il nome di una cartella e non il vero dominio (che è invece "www.konjedic.se", ma in quanti non lo notano.



Un mix di psicologia e tecnologia, con attenzione ai protocolli usati e al camuffamento del FQDN.

CONCLUSIONE

Adesso abbiamo abbastanza strumenti per scoprire un tentativo di phishing. Le tecniche si affinano ogni giorno di più, e la combinazione delle migliori può portare ad oggettive difficoltà di smascheramento.
Quindi ci sono comunque alcune dritte che ci possono aiutare a proteggerci:
Accedere ai propri siti solo via segnalibri del proprio browser (non fare "click" su quelli delle mail) Non fornire mai credenziali o informazioni personali via e-mail: nessun sito le chiede In caso di dubbio, scrivere ai contatti ufficiali del proprio sito, inoltrando il messaggio sospetto. Sarebbe utile averli già registrati nella rubrica del programma di posta, in modo da non doverli andare a cercare nel momento della "pressione psicologica" Non rispondere mai a chi vi ha mandato il messaggio sospetto.
E, sopratutto, occhi sempre attenti e cervello sempre connesso.

IMMAGINI SATELLITARI

COSA C'È DIETRO E DENTRO QUELLE BELLISSIME IMMAGINI DELLA NOSTRA TERRA CHE VEDIAMO IN POSTER E CALENDARI?

di G.ENOMA
redazione@hackerjournal.it

Di immagini satellitari ce ne sono molte, e dipendono dal soggetto ripreso. Ci sono quelle del Sole o delle stelle, quelle della radiazione cosmica di fondo e quelle della Terra. In questo articolo ci concentriamo su queste ultime, ma molti dei concetti espressi hanno una validità più generale.

Alla domanda "cos'è un'immagine satellitare della Terra" in molti risponderebbero: è quella fotografia della Terra che vediamo, ad esempio, nei poster o nei calendari.

Vero... e sbagliato. Vero perché indubbiamente quella è un'immagine della Terra vista dal satellite. Ma sbagliato perché non è quella l'immagine che il satellite ha in effetti scattato e trasferito a terra. Quindi quella che sembrava inizialmente una domanda ovvia, in realtà nasconde concetti e informazioni che racchiudono tutto un mondo invisibile ai più. Ed è quello che cercheremo di spiegare in questo articolo. Per poter entrare nello specifico, useremo come riferimento ENVISAT, satellite gestito dall'ESA (Agenzia Spaziale Europea), che grazie ai suoi numerosi strumenti a bordo e la sua notevole longevità ci permette di vedere un caso omni-comprensivo delle possibilità che potremmo incontrare.

QUALCHE CONCETTO DI BASE

Un satellite è un insieme di varie componenti che possiamo riassumere in tre grandi categorie : il payload (ovvero la struttura e i sistemi generali di funzionamento), gli strumenti scientifici, e il sistema di comunicazione da e per la Terra.

A bordo di un singolo satellite ci può essere un solo strumento scientifico o ce ne possono essere molti.

Gli strumenti possono essere di tipo più disparato, ma in generale si dividono in famiglie in funzione del tipo di parametro fisico (o di parametri fisici) che andranno a misurare. Per questo si parla ad esempio di strumenti di tipo SAR (radar), altimetrici, ottici, atmosferici, etc. I dati acquisiti a bordo del satellite sono periodicamente inviati a Terra verso le stazioni di acquisizione, sia direttamente, che tramite ponti radio con altri satelliti. Da queste stesse stazioni sono anche inviati verso il satellite i comandi necessari al suo buon funzionamento e al mantenimento della rotta corretta (inclusi quelli tutt'altro che infrequenti per evitare collisioni con altri oggetti o con immondizie spaziali).

DATI, MA QUANTI TIPI!

I dati acquisiti dal satellite e poi inviati a Terra sono di tipo "grezzo" (in termine tecnico: "raw"). Questi sono poi trasformati dalla cosiddetta "cate

Instrument / mode	Product ID	Description
ASAR	ASA_EC__0P	ASAR Level 0 External Characterization
	ASA_MS__0P	ASAR Level 0 Module Stepping Mode
WV	ASA_WV__0P	ASAR Level 0 Wave Mode
	ASA_WVI_1P	Wave Mode SLC Imagette and Imagette Cross Spectra
	ASA_WVS_1P	Wave Mode Imagette Cross Spectra
	ASA_WVW_2P	Wave Spectra Product
GM	ASA_GM__0P	ASAR Level 0 Global Monitoring Mode
	ASA_GM1_1P	Global Monitoring Mode Image (stripline)
	ASA_GM__BP	Global Monitoring Mode Browse Product (stripline)
IM	ASA_IM__0P	ASAR Level 0 Image Mode
	ASA_IMS_1P	Image Mode SLC Image
	ASA_IMP_1P	Image Mode Precision Image
	ASA_IMG_1P	Image Mode Geocoded Image
	ASA_IMM_1P	Image Mode Medium Resolution Image (stripline)
	ASA_IM__BP	Image Mode Browse Product (stripline)
AP	ASA_APH_0P	ASAR Level 0 Alternating Polarization (Xpolar H)
	ASA_APV_0P	ASAR Level 0 Alternating Polarization (Xpolar V)
	ASA_APC_0P	ASAR Level 0 Alternating Polarization (Copolar)
	ASA_APS_1P	Alternating Polarization SLC Image
	ASA_APP_1P	Alternating Polarization Precision Image
	ASA_APG_1P	Alternating Polarization Geocoded Image
	ASA_APM_1P	Alternating Polarization Medium resolution Image (stripline)
	ASA_AP__BP	Alternating Polarization Mode Browse Product (stripline)
WS	ASA_WS__0P	ASAR Level 0 Wide Swath
	ASA_WSM_1P	Wide Swath Mode Medium Resolution Image (stripline)
	ASA_WS__BP	Wide Swath Mode Browse Image (stripline)

Esempio di prodotti satellitari per uno strumento specifico del satellite ENVISAT. Si nota il nome dello strumento (ASAR), i vari modi di acquisizione (WV, GM, IM, etc.), la stringa di identificazione del prodotto (che poi è la prima parte del suo nome) e una breve descrizione dello stesso

di processamento" che li rielabora, li migliora e talvolta anche aggrega al fine di produrre il risultato desiderato. Vi sono fino a 8 livelli diversi di processamento oltre il dato grezzo, e questi sono comunemente indicati con una lettera: da L0 (elle zero, che sta per livello zero, il primo stadio di processamento del dato grezzo) a L7. Tipicamente le nostre belle immagini sono dati di tipo L2 o L3. Ciascuno di questi dati "generati" è chiamato "prodotto".

A questa differenziazione se ne aggiunge un'altra: ci sono dati di tipo NRT (Near Real Time) e OFL (Off-Line). I primi hanno la caratteristica di essere disponibili più in fretta (nel giro di pochissime ore), ma hanno una qualità inferiore, mentre i secondi sono prodotti con elaborazioni successive (sono disponibili tra 3 e 15 giorni dopo) e rappresentano lo stato dell'arte.

Per capire questa differenza qualitativa, bisogna introdurre dei nuovi "componenti" di questo processo: i file ausiliari. Si tratta di un numero variabile di file (in funzione dello strumento) che servono per aiutare il software a processare l'immagine correttamente. Ad esempio, alcuni di questi contengono informazioni sull'orbita del satellite: durante il processamento NRT il software potrà solo usare le informazioni sull'orbita "prevista", mentre quando sono prodotte le immagini nella catena OFL saranno disponibili i dati "misurati" (e quindi esatti) sull'effettiva orbita. Nei calcoli di tipo geometrico a 6 decimali, differenze tra la previsione e il dato reale, anche se minime, producono risultati diversi in modo apprezzabile.

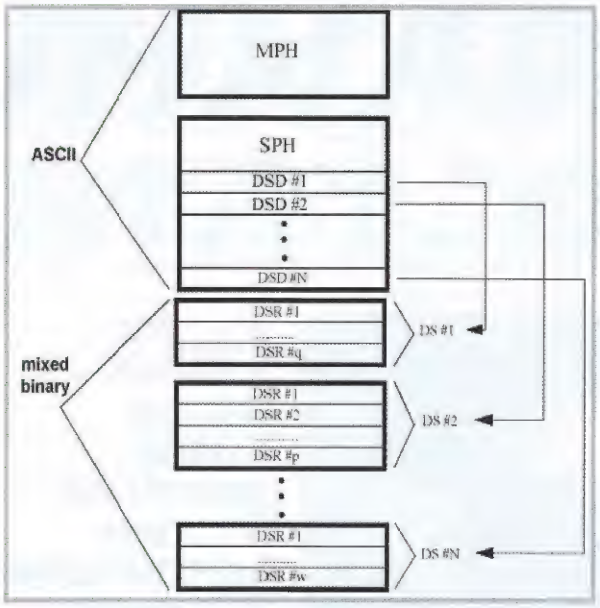
Ciascun prodotto, che sia in ingresso o in uscita, o file utilizzato durante il processamento, ha un formato documentato nei minimi dettagli. Queste specifiche si chiamano guarda caso "Product Specification" (PS). Ci sono PS anche per ciascuno dei file ausiliari. La descrizione del formato è pubblica e questo è necessario per chi deve sviluppare programmi per analizzare scientificamente, o anche solo visualizzare, i prodotti messi a disposizione degli enti che gestiscono i satelliti.

Nel caso di ENVISAT, l'insieme di tutte le specifiche è coperto da ben 18 documenti (per i link, si veda il Box riferimenti).

LA NOMENCLATURA DEI FILE

Ma tra le tante possibilità, come facciamo a sapere quali prodotti sono realmente generati? E sopratutto, dato un nome di file, come facciamo a sapere a che prodotto corrisponde? Con riferimento al nostro satellite, osserviamo il documento di cui al Rif. 1. Questo documento contiene la lista di tutti i prodotti satellitari generati, con una breve descrizione di cosa ciascuno rappresenti. Ci fornisce anche la chiave per interpretare almeno la prima parte del nome del file, quella utile ad identificare lo strumento che lo ha generato e il tipo di prodotto: Nome file= "WWW_XXX_YZ...", dove: WWW è il nome dello strumento, secondo la seguente codifica (in parentesi il nome dello strumento e il significato dell'acronimo):

ATS (AATSR: Advanced Along Track Scanning Radiometer)
ASA (ASAR: Advance Synthetic Aperture Radar)
DOR (DORIS: Doppler Orbitography and Radio-positioning Integrated by Satellite)
GOM (GOMOS: Global Ozone Monitoring by Occulation of Stars)
MER (MERIS: Medium Resolution Imaging Spectrometer)
MIP (MIPAS: Michelson Interferometer for Passive Atmospheric Sounding)
MWR (Microwave Radiometer)
RA2 (Radar Altimeter 2)
SCI (SCIMACHY: Scanning Imaging Absorption Spectrometer for Atmospheric Cartography)



Struttura dati di un prodotto ENVISAT

TLM (Housekeeping Telemetry)
WWW (codice di servizio per prodotti che contengono solo l'intestazione)

XXX è il modo in cui lo strumento sta operando o il tipo di immagine (ce ne possono essere diversi per ogni livello di processamento, ed è specifico dello strumento)

Y indica il livello di processamento:
0: Livello 0
1: Livello 1B
2: Livello 2
B: Browse (un sottoprodotto speciale)

Z indica se il prodotto è un "Parent" o Child (un estratto del parent):
P : Parent
C : Child

Per chiarezza, questa lista si riferisce solo ai prodotti, e non ai file ausiliari, che è invece definita in un altro documento della serie (Rif.2) In figura 1 potete vedere un esempio di nomenclatura dei prodotti.

LA STRUTTURA GENERICA DEI PRODOTTI

Tutti i prodotti ENVISAT seguono una struttura dati consistente, indipendentemente dallo strumento. Questa è ben descritta nel documento al Rif.3.
Se guardiamo la figura 2, possiamo vederne le componenti fondamentali:
MPH (Main Product Header): contiene le informazioni necessarie e comuni a tutti gli strumenti
SPH Specific Product Header: contiene informazioni specifiche del prodotto nel suo complesso, insieme a uno o più Data Set Descriptors
DSD (Data Set Descriptor): descrive ciascun effettivo Data Set che compone il prodotto stesso;
DS (Data Sets), l'insieme di uno o più Data Set Record
DSR (Data Set Record): l'unità di struttura atomica con cui sono riportati i dati satellitari.

IL MAIN PRODUCT HEADER

Lo MPH è in formato ASCII e quindi facilmente leggibile con un editor testuale (ma in grado di aprire file piuttosto grandi). Contiene una moltitudine di parametri interessanti (ben 41), tutti descritti in dettaglio nel documento Rif.3: dimensioni, tipo di dato, formato, significato. Senza elencarli tutti, che richiederebbe troppo spazio, possiamo evidenziarne alcuni tanto per solleticare la curiosità. Intanto il nome per intero del prodotto (noi abbiamo visto solo i primi, ma il nome intero è lungo ben 62 caratteri). Poi abbiamo la stazione dove è stato acquisito a Terra, informazioni su data e ora di inizio e fine dell'immagine, sull'orbita e posizione del satellite, tipo di prodotto (NRT o Offline, o altro), la stazione dove è stato processato e quando ciò è avvenuto. Abbiamo anche il documento di riferimento per la struttura del prodotto: nel tempo le specifiche si aggiornano ed è importante sapere a quale versione il nostro prodotto si conforma.
Ci sono anche informazioni sulle dimensioni del prodotto, delle varie strutture (SPH, DSD, etc) che lo compongono e le quantità in cui esse appaiono, in modo da poterle leggere correttamente.
Insomma, una vera miniera. In figura 3 potete osservare un esempio di MPH. A voi l'esercizio di decodificarlo...

LO SPECIFIC PRODUCT HEADER

Quello che lo MPH fa a livello generale, lo SPH lo fa specificatamente per il tipo di strumento e prodotto.
Questa prima parte è specifica di ciascuno strumento, e per come sono definite le Product Specification di ENVISAT è contenuta in file separati (ad esempio Rif.4 per lo strumento MIPAS).
Ma quello che più ci interessa è che fornisce una sorta di indice per i DSD.

IL DATA SET DESCRIPTOR

Abbiamo visto in figura 2 che essi sono usati per descrivere le strutture dati contenute nel prodotto. In realtà osservandoli ci si accorge che questo indice punta a due diversi tipi di informazioni:

Esempio di MPH (Main Product Header). Si nota che è in formato ASCII e quindi facilmente leggibile

```
DS_NAME="SR/GRØADSØØØØØØØØØØØØØØØØØØØØ"
DS_TYPE=A
FILENAME="ØØØØØØØØØØØØØØØØØØØ
```

N	Description	Units	Byte Length	Data Type	Dim
1	Number of days elapsed since the 1st of January 2000 at 0:0 hour. It may be negative, and is thus a signed long integer	days	4	sl	1
2	Number of seconds elapsed since the beginning of that day	s	4	ul	1
3	Number of microseconds elapsed since the last second	µs	4	ul	1
TOTAL			12		

Struttura del formato di data MJD 2000 – Modified Julian Day 2000 – usato per il timestamp all'interno dei DSR

10:00 sarà codificato come {-2, 36000, 0} (10 ore = 60x60x10 secondi).

CONCLUSIONE E RIPARTENZA

Ora abbiamo tutti gli strumenti per procedere con la nostra investigazione e sperimentazione. O anche (perché no?) magari iniziare un progetto OpenSource per un software di processamento, o analisi o solo visualizzazione di immagini satellitari. Al momento gratuiti ce ne sono pochi (e spesso solo per visualizzazione), mentre quelli per il processamento sono proprietari e costosi. Spesso chi sviluppa è più uno scienziato che un geek che mangia bit a colazione, e li mangia in parallelo sulle due arcate per ottimizzare la masticazione e non sprecare "cicli di crock". :-) Il processamento è molto pesante e quindi la sfida è difficile: fare qualcosa di migliore, più veloce, più stabile, più open ai contributi di tutti, più... insomma la vera qualità hacker, senza compromessi. Qualcosa che integri lo stato dell'arte in termini di processamento distribuito, modularità, facilità d'uso, condivisione di risorse (qualcuno ricorda SETI o BOINC?). Le immagini satellitari sono fatte per monitorare il nostro ambiente: sarebbe bello coinvolgere persone sparse ai 4 angoli della Terra, con competenze diverse (perché anche gli scienziati servono...) intorno ad un progetto per il beneficio di tutti...

Documenti referenziati

Ecco i dettagli dei documenti referenziati nel testo

Sito web in cui trovarli: http://earth.esa.int/pub/ESA_DOC/ENVISAT/index.htm

Notate che il nome del file contiene la sua versione: quelle elencate qui sono le versioni al momento in cui scriviamo:

Rif.1: vol04_3c.products_overview.pdf - ENVISAT Products Specifications - Volume 4: Products overview

Rif.2: Vol16_Aux_data_files_3g.pdf – ENVISAT Products Specifications - Volume 16: Auxiliary Data files

Rif.3: Vol05_Structures_3d_20071122.pdf - ENVISAT Products Specifications - Volume 5: Product Structures

Rif.4 Vol12_Mipas_4C.pdf - ENVISAT Products Specifications - Volume 12: MIPAS Products Specifications

A ME GLI OCCHI

IL SOCIAL ENGINEERING È UNA DELLE FORME DI "ATTACCO" PIÙ SUBDOLE PERCHÉ VA A COLPIRE UN BERSAGLIO SPESSO COMPLETAMENTE PRIVO DI DIFESE: L'UOMO.

di N. Bassetti - redazione@hackerjurnal.it

Nonostante la sempre maggior raffinatezza, dal punto di vista tecnico, dei programmi malware odierni, i cybercriminali cercano spesso di sfruttare proprio le debolezze "umane", al fine di realizzare la diffusione su larga scala dei programmi maligni da essi elaborati. Ciò non dovrebbe, in ogni caso, sorprenderci più di tanto. Gli esseri umani costituiscono in effetti, di solito, l'anello più debole all'interno di qualsivoglia sistema di sicurezza. Il Social Engineering (Ingegneria Sociale) è proprio l'arte di persuadere qualcuno a collaborare, a fornire informazioni riservate, questa pratica si realizza con una pianificazione ben precisa ed attacca l'interfaccia umana di un sistema informativo protetto. Il Social Engineering funziona a causa della caratteristica umana di fidarsi delle altre persone, le quali hanno la tendenza a simpatizzare con qualcuno che sostiene di essere in difficoltà o a credere a chi millanta di essere una persona meritevole di fiducia (es. ricoprendo un ruolo specifico, una carica, un titolo, ecc.), senza prima controllare le credenziali. Un ingegnere sociale, lo sa e anticipa questo.

STUDIARE L'AVVERSARIO

Un primo step per sferrare l'attacco "sociale" è reperire più informazioni possibili sull'obiettivo (footprinting) da colpire, gli indirizzi, i

numeri di telefono/fax, le e-mail, account di messaggistica/Skype, di che cosa si occupa, le sedi distaccate, il sito web, i nominativi di chi ci lavora, ecc. ecc.
Raccolte tutte queste informazioni, si cerca di capire che cosa si vuol raggiungere e come farlo. Lo studio approfondito del "bersaglio" serve anche a prepararsi le risposte ad eventuali domande di controllo da parte del personale preposto.

Il sito Get Safe Online mette a disposizione guide e consigli pratici di facile attuazione per una navigazione sicura su internet.

GLI APPROCCI

Supponiamo di voler accedere ad un'area riservata condivisa su web di un'azienda, l'ingegnere sociale, potrebbe tentare, con appunti alla mano del precedente footprinting, un approccio telefonico, spacciandosi per un sistemista di una sede distaccata, lamentando l'impossibilità di accedere all'area riservata e chiedendo cortesemente la password o il numero di telefono di un responsabile. Nel fare tutto questo bisogna cercare di rimanere il più possibile "invisibili", il che significa non lasciare tracce nella memoria dell'interlocutore, come ad esempio, accenti marcati, toni vocali particolari, insomma diventare "l'uomo qualunque". Con la stessa tecnica, ci si può spacciare per l'impiegato, utente, fornitore, cliente, imbranato e/o incompetente, come un tecnico dell'azienda che fornisce l'hosting, in questo caso si può "rimbambire" una persona NON tecnica dell'azienda, usando un frasario stregonesco-informatico, in modo da acquisire la sua fiducia e farsi rivelare ulteriori informazioni.

I sistemi più usati sono:

• **Il telefono** – conversazioni telefoniche dalle quali trarre informazioni. Quante volte si forniscono dati a chissà chi pensando che sia un cliente o un fornitore? Un esempio può essere quello di dettare una password ad un fantomatico cliente che lamenta lo smarrimento della stessa.

• **Online** – Il meccanismo è lo stesso di quello telefonico, solo che il mezzo cambia. Questo tipo di attacco può essere sferrato tramite e-mail, chat, VoiP, ecc. Un esempio può essere quello di "forgiare" una finta e-mail, che riporta un mittente fidato (come accade per il famigerato phishing), quindi l'operatore in tutta tranquillità risponde alla mail fornendo le informazioni richieste.

• **La spazzatura (Dumpster diving)** – Uno dei sistemi più "classici", cercare appunti, post-it e quant'altro sia utile a ricavare nomi, indirizzi, numeri, password, ecc. Nel cestino della spazzatura.

• **Shoulder surfing** – Questa è una tecnica che può far sorridere, ma a volte funziona! Mettersi alle spalle di qualcuno e spiare ciò che scrive sul PC.

• **Reverse social Engineering** - Questa è una tecnica raffinata, poiché grazie ad una relazione , precedentemente instaurata, l'attaccante riesce a farsi contattare dalla propria vittima, che è in completa balia del truffatore. Si possono fare vari esempi, come quello di spacciarsi per un servizio tecnico relativo alla connettività, di lasciare un recapito (e-mail, telefono, ecc.) per farsi contattare nel momento del bisogno. Poi effettuare un "sabotaggio" alla connettività della vittima, in modo tale da farsi chiamare, con la scusa dell'assistenza remota, ci si può far dare username, passwords, indirizzi IP, ecc. ecc.

• **La persuasione** – Questo è un tipo d'attacco basato tutto sulla capacità recitativa dell'attaccante, lo vediamo spesso nella cronaca e nella vita. In parecchie città sono stati segnalati degli individui che riuscivano a spacciarsi per amici di un

La scelta delle password

A volte, per non complicarsi troppo la vita, le persone sono solite prendere delle scorciatoie, non comprendendo magari a dovere, ad esempio, tutte le implicazioni legate all'adozione di adeguate misure di sicurezza online. Ed è proprio ciò che avviene spesso con la scelta delle password. Le operazioni online condotte dagli utenti della Rete si infittiscono oramai sempre di più: shopping, transazioni bancarie, pagamenti di bollette, networking professionale, e molto altro ancora. Di conseguenza, non è affatto raro il dover a volte gestire, ad esempio, 10, 20 o più account online; ciò rende ovviamente estremamente difficile ricordare (o addirittura semplicemente scegliere) una password univoca per ogni account. Per tal motivo si è in genere molto tentati dall'utilizzare la stessa password per ogni account in essere, così come il nome di un bambino, del proprio coniuge o di una località che abbia per noi un particolare significato, ovverosia un nome che possa essere agevolmente ricordato. Un altro approccio comune è quello di riciclarsi le password, magari utilizzando qualcosa del tipo 'mionome1', 'mionome2', 'mionome3', e così via per tutti gli account successivi. Agendo in tal modo, tuttavia, aumenta considerevolmente la probabilità che un cybercriminale possa riuscire nell'intento di impadronirsi della nostra password e, qualora il nostro account venga violato, il malintenzionato di turno potrà così ottenere un facile accesso ad ulteriori nostri account online. L'eventualità di correre un rischio del genere rimane tuttavia ben lungi dall'essere adeguatamente considerata da quella parte del personale aziendale non in possesso di specifiche conoscenze tecniche, così come dal pubblico generico della Rete. E, anche nel caso in cui si sia a conoscenza dei potenziali pericoli esistenti, rimarrà pur sempre arduo poter intravedere una qualche valida alternativa a tutto ciò, dal momento che non è

identitytheft.org.uk dà consigli in materia di sicurezza Internet.

familiare della vittima e a farsi consegnare del denaro. Questi utilizzano tecniche di PNL (Programmazione Neuro Linguistica), sanno farsi dare delle informazioni facendo credere esattamente l'opposto, possiamo fare un esempio banale:

Attaccante: "Salve si ricorda di me?"
Vittima: "No …dove ci siamo conosciuti?"
Attaccante: "Sono un ex compagno di scuola di suo figlio…[pausa]"
Vittima: "Di chi di Mario o di Luigi?"
Attaccante: "di Mario, a proposito come sta?"
Vittima: "Bene sta studiando all'università, ci sta mettendo un po', se la prende comoda lui!"
Attaccante: "Ahahahahah me lo ricordo è sempre stato uno scansafatiche…bene son contento, io ho dovuto lasciare invece…purtroppo"
Vittima: "ah! Come mai?"

E poi parte una storia strappalacrime, che persuade la vittima a lasciare dei soldi al poverino. Ma chi era costui?

La stessa tecnica può essere adottata al telefono, spacciandosi con estrema sicurezza come qualcuno del comparto tecnico, che necessita di parlare col responsabile dell'area amministrativa e di lì convincerlo a cedergli le credenziali d'accesso al sistema informativo.
Un altro esempio:
Presentarsi presso un'azienda come candidato ad un colloquio di lavoro, chiedere dove sia la macchinetta del caffè e subito dopo tornare col curriculum cartaceo sporco della nera bevanda, a questo punto, chiedere gentilmente ad un operatore dell'azienda se può fargli stampare una copia del curriculum prendendola dal pendrive dell'attaccante.
Non tutti sanno che si può inserire un software autopartente nei pendrive USB, che preleva tanti dati (password delle email, password memorizzate nelle sessioni di navigazione, ecc.), senza che l'operatore se ne accorga, il gioco è fatto!

LE CONTROMISURE

La formazione e le procedure sono le contromisure più efficaci per combattere gli ingegneri sociali, le procedure possono essere la classificazione dei dati (con i vari livelli d'accesso) e la conservazione e lo smaltimento dei dati (smaltire in modo sicuro e conservare al sicuro).
La formazione al personale deve essere in grado di far lavorare tranquillamente il personale, ma renderlo abbastanza scaltro e scettico al fine di non incorrere nelle trappole del truffatore. Chiaramente ogni reparto aziendale avrà una formazione ad hoc, profilata sul tipo di operatività in essere, ad esempio l'Help Desk non può essere brusco o freddo nei confronti dei chiamanti, deve riuscire a mantenere l'affabilità e la gentilezza corazzate da un sano scetticismo ed attenzione. Insomma alcune regole di base ci sono.

CONTROLLARE SEMPRE LE CREDENZIALI DI TUTTI

Avere delle politiche aziendali di sicurezza (non inserire pendrive esterni, non lasciare dati in vista sia sui monitor sia su cartaceo, distruggere la spazzatura contenente dati, ecc.) Evitare di fornire informazioni a chi le richiede via e-mail o telefono, nessun operatore serio chiederà mai password, numeri di carte di credito, ecc. via remota, questo genere d'informazioni vanno riferite di persona o con dei mezzi sicuri. Effetture periodicamente dei test con delle simulazioni o dei giochi di ruolo. Classificare le informazioni e cercare di capire a chi potrebbero interessare e come potrebbero essere usate. Imparare a contrastare il Social Engineering non serve solo in ambito aziendale, ma anche nella vita quotidiana di ognuno di noi, alla fine le truffe son sempre esistite, sono solo cambiati i mezzi.

affatto semplice potersi ricordare agevolmente 10, 20 o più password.
Eppure esiste una soluzione per l'annoso problema delle password! Anziché cercar di ricordare ogni singola password, si può porre quale base un componente fisso, per poi applicare una particolare formula atta a ben "mescolare" le carte in tavola. Ecco un esempio; partendo dal nome della risorsa on-line, ad esempio 'mybank', si applica la seguente formula:

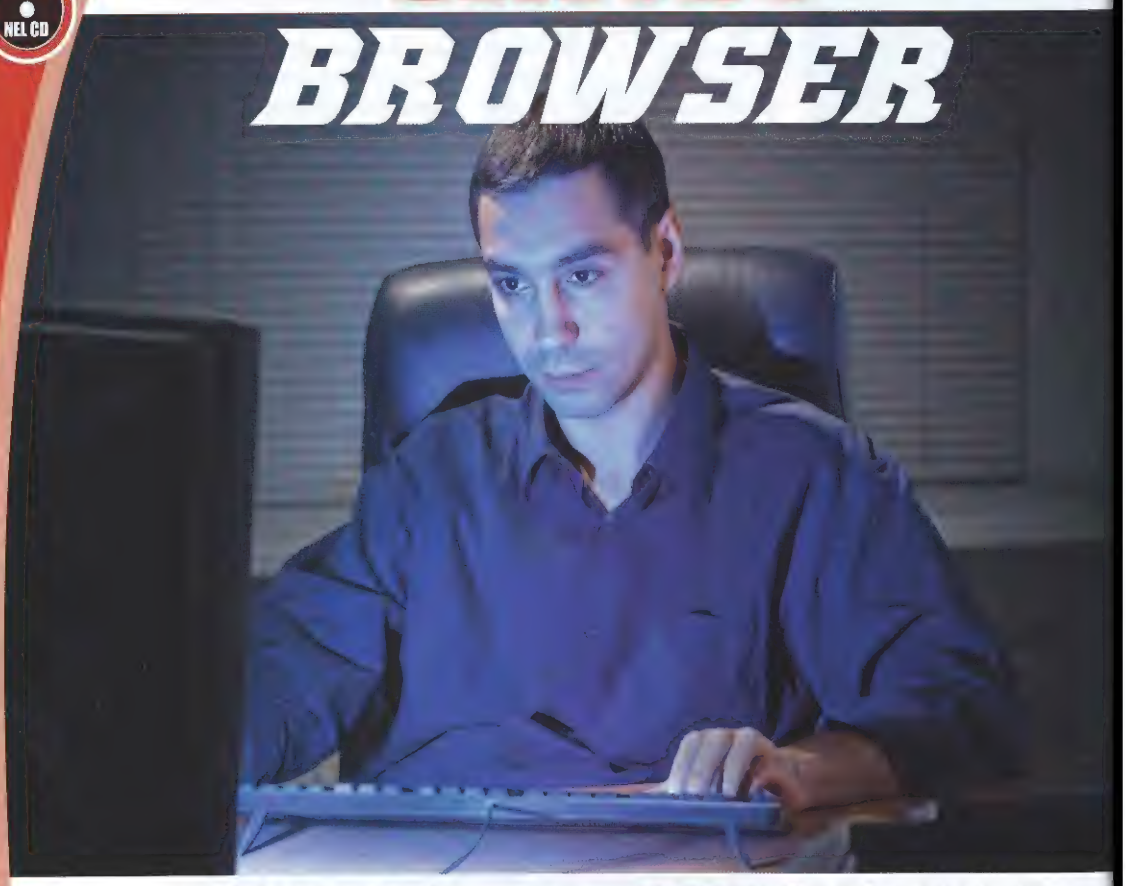
Scrivere in maiuscolo la quarta lettera.
Collocare la penultima lettera all'inizio.
Aggiungere un numero a scelta dopo la prima lettera.
Aggiungere un carattere non alfanumerico a scelta alla fine della password.
Si può così ottenere una password del genere: 'n1mybAk;'. Avvalendoci di tale metodo, ovverosia seguendo e ripetendo ogni volta i quattro passi sopra enunciati, avremo una password univoca per ogni account online di cui disponiamo.

Risorse anti social engineering
Esistono già numerosi siti web che dispensano utilissimi consigli in materia di sicurezza Internet. Citiamo, tra di essi, Get Safe Online, identitytheft.org.uk e Bank Safe Online. Inoltre, le aziende produttrici di soluzioni per la sicurezza online sono in genere solite mettere a disposizione degli utenti delle vere e proprie guide per garantire la navigazione sicura in Internet, quali, ad esempio, la Guide to stopping cybercrime di Kaspersky . Esse forniscono, tutte quante, validi consigli e dispensano efficaci norme comportamentali per salvaguardare al meglio le attività online degli utenti, nell'intento di ridurre al minimo il rischio di cader vittima di criminali informatici. Tuttavia, per poter procedere alla consultazione delle stesse, è ovviamente condizione indispensabile l'essere connessi ad Internet.

INTERNET

NEL CD

CRAZY BROWSER



LEGGERO E VERSATILE, UN BROWSER IN GRADO DI SODDISFARE OGNI UTENTE.

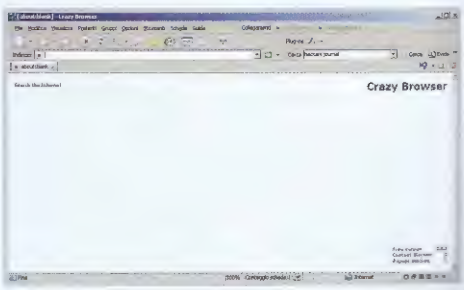
di Massimiliano Brasile
redazione@hackerjournal.it

Quante volte ci capita di voler aprire una pagina al volo, perché abbiamo poco tempo oppure perché abbiamo dimenticato di guardare un'informazione e anche il tempo di caricamento di Internet Explorer o Firefox possono essere fastidiosi?

O magari abbiamo un vecchio computer che può ancora dare soddisfazioni, ma che per scarsa memoria o processore un po' lento, fatica ad aprire i siti web fatti solo per chi ha la banda larga. Per questi problemi e anche per chi vuole una soluzione semplice ed efficiente, è stato creato Crazy Browser un leggerissimo browser web che non ha nulla da invidiare ai big del settore. Anzi, forse ha nella sua estrema leggerezza un valore aggiunto che ormai gli altri hanno perso.

CARATTERISTICHE

Crazy Browser è completamente freeware e animato da un puro spirito non-profit. Questo ne fa un candidato perfetto ad esempio per laboratori informatici di scuole e centri di aggregazione che solitamente hanno a disposizione computer non nuovissimi.

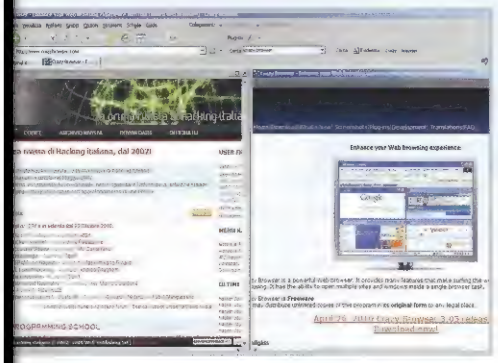


Quando lanciamo Crazy Browser siamo accolti da un'interfaccia minimale che ricorda molto Chrome con solo una barra per lanciare una ricerca in rete, in basso possiamo vedere la versione in uso.

Il file di installazione occupa poco più di 700kb e può quindi stare benissimo anche sui vecchi floppy-disk. Una volta installato supera di poco il megabyte. Si tratta comunque di un browser di tutto rispetto che supporta il multithread (possono quindi essere aperte più pagine contemporaneamente) e la sua interfaccia è personalizzabile. Grazie al lavoro di traduzione di Giacomo Margarito è poi disponibile anche in italiano: basta decomprimere l'archivio italian.zip nella cartella \ Programmi\Crazy Browser\Languages, riavviare Crazy Browser e selezionare dal menu View ☒ Languages ☒ Italian).

Crazy Browser è pronto per tutte le moderne tecnologie, oltre quindi a javascript (e la soppressione degli errori), c'è il pieno supporto per flash e java e nessun problema per i recenti plugin come SilverLight. E' in grado di gestire inoltre la visualizzazione con più monitor, utile per i fortunati che possono goderne.

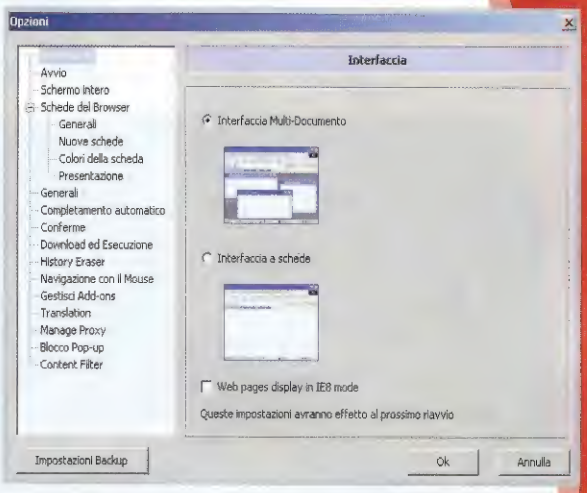
E' inoltre integrato un blocco automatico di finestre pop-up (solitamente pubblicitarie) che permette comunque di essere personalizzato in base al sito che si sta visitando; a questa funzione si può associare una funzionalità "intelligente" che attinge da database condivisi sui siti di spam per bloccare preventivamente l'apertura di pagine e finestre con contenuti non voluti. Utile poi la funzione che permette di salvare più pagine insieme per riaprirle al prossimo riavvio, sullo stile di Firefox. Anche i motori di ricerca possono essere personalizzati, ma di base Crazy Browser dispone già dei link più famosi. E sono supportati anche i plugin (COM Objects, Script ed eseguibili esterni). Sono supportati i protocolli di sicurezza SSL (utilizzati per home-banking ed e-commerce ad esempio) ed è possibile scegliere la modalità di visualizzazione delle finestre: in stile tab, o come finestre multiple incluse (sullo stile di Opera).



Con un click sui bottoni in basso a destra possiamo organizzare in un attimo le finestre o tab che abbiamo aperto; questo ci permette di tenere sempre in ordine i siti che visitiamo senza perderci in infinite pagine.

Crazy Browser risulta davvero semplice da utilizzare, adottando un'interfaccia pulita che ricorda molto da vicino Internet Explorer (sia per lay-out che grafica delle icone). Scelta che sicuramente può andare incontro a quegli utenti poco avvezzi ai cambiamenti e che poi faticano a trovare la disposizione delle funzioni a essi familiari. Altra caratteristica che va in questa direzione è rappresentata dai tab che si aprono al posto delle nuove finestre: quando apriamo un nuovo link, i tab non tolgono automaticamente il focus dalla pagina che stiamo guardando, evitando lo stress ottico per chi apre molte pagine insieme e in generale abbiamo davvero tutto lo spazio dedicato alla pagina web. Per riorganizzare poi tutte le finestre aperte abbiamo anche comodi pulsanti in basso a destra.

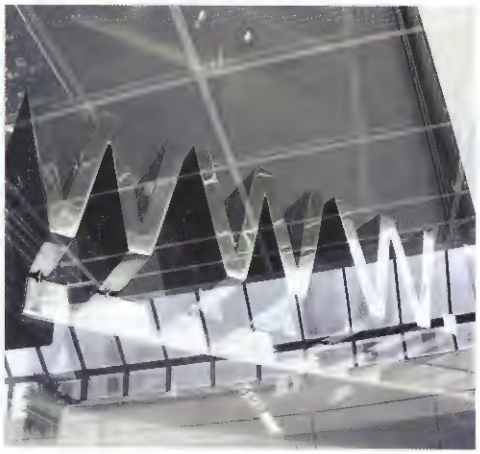
GIUDIZIO



Nelle opzioni avanzate abbiamo la possibilità di personalizzare ogni aspetto di Crazy Browser, ma se non siamo interessati abbiamo comunque uno strumento valido già pronto e semplice da usare.

Grazie a un lavoro davvero egregio, sono state pescate funzionalità presenti nei browser più utilizzati e sono state implementate in un motore molto leggero che non ci farà certo rimpiangere di aver dimenticato un plugin o una estensione. Considerando il supporto per tutte le tecnologie più largamente utilizzate dai siti web, è sicuramente un prodotto alla portata di chiunque che permette di ottenere ottime prestazioni anche su hardware più datati. Senza quindi dover agire su vecchi PC e metter mano al portafogli per eventuali upgrade, è possibile godere della navigazione web da subito con un prodotto affidabile e gratuito.

Da provare anche per chi non ha problemi a usare ogni giorno i più blasonati browser.



IL FIREWALL IN UN FLOPPY

BASTANO 1,4 MB PER AVERE A PORTATA DI MANO UN FIREWALL AFFIDABILE. NON CI CREDETE? CHIEDETE AL "COYOTE".

di Spirit
redazione@hackerjournal.it

Con un semplice dischetto da 1.4MB si può avere un firewall che protegge bene la propria LAN da accessi indesiderati provenienti da Internet. Con un CD-ROM si possono aggiungere letteralmente centinaia di strumenti per gestire il proprio firewall e mantenere la propria rete senza problemi. Il tutto grazie ad un Firewall che definire "tascabile" è davvero poco: Coyote! Al momento sono disponibili diverse versioni di firewall di Linux live che si possono scaricare all'indirizzo www.coyotelinux.com. La particolarità di Coyote, quella che fa notizia, è l'avvio da floppy disk, però, considerando che il floppy sta lentamente scomparendo dal panorama informatico sul sito è disponibile un'ISO da masterizzare su CD per consentire l'avvio da questa unità.

UN FIREWALL CON COYOTE LINUX

Usando un solo, semplice script, Coyote Linux permette di creare un firewall Linux di lancio in grado di entrare su un floppy disk. Una volta che Coyote Linux viene installato e lanciato, può essere tranquillamente gestito da un altro computer sulla LAN. Si può usare una interfaccia Web o ci si può collegare usando ssh e gestendo Coyote Linux da una shell di Linux. Coyote Linux contiene un incredibile numero di funzionalità per un ingombro così ridotto. Dopo aver lanciato il floppy di boot di Coyote Linux creato, si ha un firewall con cui si può:

- Instradare pacchetti tra la LAN e Internet
- Fornire interfacce di rete alla LAN Ethernet (TCP o PPPoE) o alle connessioni dialup (PPP).
- Creare regole di firewall supportate da iptables (Si inizia con poche semplici regole, ma si possono aggiungere le proprie regole per includere IP Masquerading e NAT, reindirizzamento di porte, trasparent proxy o molte altre funzionalità di iptables).
- Attivare DHCP. Coyote Linux può funzionare come un server DHCP, fornendo indirizzi IP e altre informazioni ai computer sulla LAN.
- Tracciare l'attività. Oltre a registrare i log delle attività sul firewall, Coyote può essere impostato per inoltrare i log a un altro computer sulla LAN.
- Controllare le attività di rete. Ci sono alcuni strumenti amministrativi di base su Coyote Linux per un controllo basilare della rete. Questi strumenti includono traceroute e nslookup.
- Collegarsi da remoto (ssh) e utilizzare la shell. Il demone sshd in Coyote Linux per-

mette di collegarsi da un altro computer alla LAN. L'utility busybox fornisce un buon set di strumenti base per la shell.

• Aprire un'interfaccia Web verso Coyote Linux. Da qualsiasi Web browser sulla LAN si può aprire l'interfaccia Web di amministrazione di Coyote Linux digitando l'indirizzo IP del proprio firewall e la porta 8180 (per esempio http://192.168.0.1:8180).

Una volta che si ha il firewall Coyote Linux in funzione, è possibile cambiare le regole del firewall da un altro computer sulla LAN, usando un Web browser o l'interfaccia shell (SSH) del computer. Se si conoscono le funzionalità della shell e del firewall si possono realizzare molte cose con questa piccola e "deliziosa" distribuzione, come routing, connessione su richiesta, e usare un servizio DHCP.

Nota: Per ulteriori informazioni, si può consultare il sito Web di Vortech Consulting, LLC (www.vortech.net). Sono i creatori del progetto Coyote Linux. Come molte compagnie che sostengono i software open source, offre prodotti commerciali collegati al progetto open source. Se si vogliono prodotti avanzati e supporto, si può considerare l'acquisto dei loro firewall dedicati alle piccole e grandi aziende.

CREARE IL FLOPPY

I requisiti di sistema e "fisici" per creare il floppy con il firewall Coyote Linux sono i seguenti:

• Floppy drive - sarà necessario un computer con un floppy drive per scrivere i dati. Sulla macchina dovrebbe girare Linux (se non si è già installato Linux, una distribuzione come KNOPPIX dovrebbe andare bene).

• Boot da floppy - Per questo, è necessario un computer che possa partire dal floppy e che abbia due interfacce di rete. Il computer può anche avere la minima potenza di un vecchio 486. Nell'esempio, il computer con il firewall avrà bisogno di un modem dial-up per connettersi ad Internet e di una scheda Ethernet per collegarlo alla LAN (anche se è molto più semplice avere una connessione Ethernet ad Internet che, fondamentalmente, può attivarsi automaticamente nella maggior parte dei casi).

E, naturalmente, sarà necessario un floppy disk:

Il computer con cui sarà creato il floppy disk e il computer su cui questo sarà fatto girare, potranno (non necessariamente) essere lo stesso. È tuttavia necessario sapere il nome del driver Linux per la scheda Ethernet prima di iniziare la procedura per creare il floppy del firewall. Se non si sa quale sia, si raccomanda di lanciare KNOPPIX sulla propria macchina e poi usare i comandi lsmod e lspci per scoprire i nomi dei driver per le schede Ethernet (dovrebbero essere state rilevate automaticamente). Usare modinfo se non si è sicuri che il nome del driver sia quello corretto (per esempio, modinfo 8139too).

Se possibile, è consigliabile utilizzare una connessione a banda larga o un'altra interfaccia Ethernet per collegarsi ad Internet perché i modem dial-up potrebbero aver bisogno di essere configurati, hanno una connessione lenta, e la connessione cade spesso. Diciamo che anche se la connessione dial-up non si usa praticamente più, lo scopo di questo articolo è soprattutto didattico e vuole dimostrare come i sistemi Linux siano così scalabili da adattarsi anche a risorse di sistema e di rete davvero minime.

Per creare un firewall con Coyote Linux, bisogna seguire questi passaggi:

1. **Su un computer che ha un lettore CD e un lettore di floppy,** copiare la directory Coyote Linux sull'hard drive del proprio computer. Aprire poi una finestra di terminale (o altra shell) e spostarsi su quella directory.

2. **Decomprimere ed estrarre il file Coyote Linux** digitando quanto segue:

```
# tar xvfz coyote*tar.gz
```

3. **Spostarsi nella directory coyote appena creata e lanciare lo script makefloppy.sh** per creare il floppy disk di Coyote Linux, come segue:

```
# cd coyote
# ./makefloppy.sh
Coyote floppy builder script v2.9
Please choose the desired capacity
for the created floppy:
1) 1.44Mb (Safest and most reliable
but may lack space needed
for some options)
2) 1.68Mb (Good reliability with extra space) - recommended
3) 1.72Mb (Most space but may not
work on all systems or with
all diskettes)
```

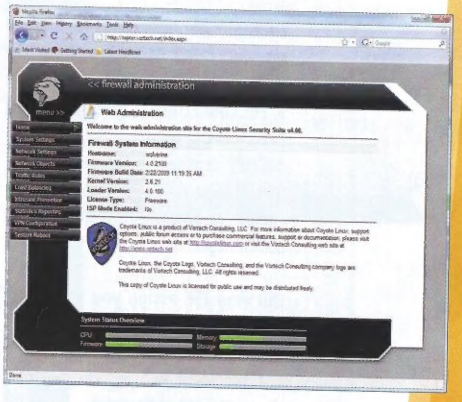
4. **Selezionare la capacità del proprio floppy disk.** In questo caso è stata selezionata la 3 (1.72MB) e ha funzionato bene. Con un vecchio floppy drive, potrebbe essere necessario utilizzare una minore capienza, il che includerà un minor numero di funzionalità.

```
Enter selection: 3
Please select the type of Internet
connection that your
system uses.
1) Standard Ethernet Connection
2) PPP over Ethernet Connection
3) PPP Dialup Connection
```

5. **Questo esempio utilizza una connessione dial-up PPP,** quindi digitare 3:

```
Enter Selection: 3
.
.
.
By default, Coyote uses the following
settings
for the local network interface:
IP Address: 192.168.0.1
Netmask: 255.255.255.0
Broadcast: 192.168.0.255
Network: 192.168.0.0
```

Nota: Se si utilizza una connessione Internet a banda larga (DSL, modem via cavo o alta Ethernet), solitamente a questo punto si seleziona 1. Selezionare 2 se l'ISP ha comunicato che si ha una connessione PPPoE. Configurare una connessione Ethernet, in realtà, è più semplice che configurare una connessione dial-up. Invece di definire il dialer, basta solitamente definire la connessione Internet via DHCP e inserire il nome dell'host (quando richiesto).



6. **Si può semplicemente accettare l'indirizzo IP di default** (e i Netmask, Broadcast e numeri di rete connessi), digitando N. Se si sta creando un nuovo set di indirizzi per la propria LAN, un set comune di indirizzi IP da usare è questo (192.168.0.1, 192.168.0.2, e così via). Si prenda in considerazione la possibilità di

cambiare l'indirizzo IP se entra in conflitto con la numerazione di rete presente o se quel set di indirizzi IP è in uso sulla propria interfaccia in Internet.

Would you like to change these settings? [Y/N]: N
OPTIONS CONFIGURATION
Demand Dial:
Initiate the link only on demand, i.e. when data
traffic is present.

7. Ora si possono creare le funzionalità di dial-up (se si sta usando una connessione dial-up per accedere a Internet, come nell'esempio). La prima domanda è se acconsentire alla connessione su richiesta (Demand dialling). Selezionale y se si desidera che la connessione Internet parta ogni volta che qualcuno tenti di aprire una connessione a quell'interfaccia (per esempio tentando di navigare il Web o di spedire una e-mail dal sistema locale o qualora un computer sulla LAN la utilizzi come via d'accesso a Internet).

Do you want to enable the demand dial option [y/n]: y

8. Inserire dopo quanti secondi di idle (l'intervallo di tempo durante il quale nessun dato passa sulla connessione di rete) la connessione dial-up a Internet verrà interrotta. L'intervallo di default è 180 (tre minuti). In questo caso è stato cambiato a 600 (10 minuti)

Enter number of seconds for idle disconnect [180]: 600

9. Per connettersi a Internet con un determinato indirizzo IP (assegnato dall'ISP), digitare y e aggiungere l'indirizzo IP come richiesto. In molti casi, comunque, si avrà l'indirizzo IP assegnato dall'ISP digitando n.

Did your ISP assign you a static IP ADDRESS? [y/n]: n
Setting up for dynamic PPP Address
Set the local PPP interface IP address. Should not be the
same as 192.168.0.1, but on the same subnet.

10. Si necessita di un indirizzo IP iniziale per far partire l'interfaccia PPP. Come visto, si dovrebbe usare un indirizzo IP presente sulla medesima rete LAN.

Dalla scheda logging si possono settare i parametri di configurazione di Coyote.

Press enter for [192.168.0.3]: 192.168.0.3

11. Le molteplici domande qui sotto sono relative al settaggio della connessione dial-up. Il dispositivo tty è la porta seriale cui è collegato il modem (ttyS0 per COM1, ttyS1 per COM2, e così via). La velocità della porta indica quanto velocemente il computer può comunicare col modem (il default, 115200, va bene). ATZ è lo script comune per l'inizializzazione del modem (fare riferimento al manuale per l'uso del modem se si necessitano ulteriori informazioni). Inserire un nome che descriva il proprio ISP (senza spazi). Inserire il numero di telefono cui collegarsi per connettersi a Internet. Infine, inserire il nome utente e la password forniti dall'ISP per l'account Internet in questione.

Enter tty device name for modem (ttyS0, etc)[ttyS0]: ttyS0
Enter ttyS0's port speed (115200, 57600, etc)[115200]: 115200
Enter modem init string (Enter = ATZ): ATZ
Enter name of ISP (no whitespace) [isp]: att
Enter phone number to dial: 5551212
Enter username: jsmith
Enter password: tkN0stf

12. Inserire n per non inviare password in chiaro durante il login. Potrebbe essere necessario inserire y se l'ISP richiede un'autenticazione CHAP o PAP.

If you enable this, your password will be sent in clear
text over the line. Say yes here only if despite having
verified everything, you still cannot connect to your ISP.
Login during chat? [y/n]: n

13. Dato che il firewall in esempio fornirà indirizzi IP agli altri computer sulla LAN, deve essere abilitato come server DHCP (y). Si faccia poi una lista della gamma di indirizzi che questo può assegnare a quei computer. Se si pianifica di avere sulla LAN 100 computer o meno, la gamma di indirizzi nell'esempio dovrebbe funzionare bene:

Do you want to enable the coyote DHCP server? [y/n]: y
Enter DHCP range starting IP [192.168.0.100]: 192.168.0.100
Enter DHCP range ending IP [192.168.0.200]: 192.168.0.200

14. Il DMZ serve a proteggere ulteriormente la rete locale dal mondo esterno se si vuole avere un Web server protetto dallo stesso firewall. In questo caso, è possibile aggiungere un'altra scheda Ethernet al firewall, connetterla al Web server e poi autorizzare il passaggio delle richieste di servizi Web in entrata attraverso il Web server. Questo permetterà di continuare a bloccare tutto il traffico in entrata ai sistemi desktop sulla propria LAN. Per questo esempio, si è scelto semplicemente N.

If you don't know what a DMZ is, just answer NO
Would you like to configure a De-Militarized Zone? [Y/N]: N

15. Determinare il nome di dominio cui sarà associato il firewall e inserire l'indirizzo o gli indirizzi IP dei server DNS che questo userà per risolvere gli indirizzi (probabilmente forniti dall'ISP, a meno che non si stia facendo girare un proprio server DNS):

```
Enter Domain Name: example.com
Enter DNS Server 1: 123.45.68.799
Enter DNS Server 2 (optional):
123.45.68.800
If you have a syslog server on your
LAN you want Coyote to
send its syslog data to, you can spe-
cify the address here.
If unsure or you do not have a syslog
server, leave this
entry blank.
```

16. Coyote può registrare le proprie attività su un altro server nella rete. Questa caratteristica può essere molto utile perchè rimuove i log dal firewall (in modo che nessuno possa alterarli) e abilita l'amministrazione centrale dei log sulla rete. Prima che sia possibile utilizzare questa funzionalità, è necessario configurare il supporto per l'accesso remoto al proprio computer di log. Per disabilitare la funzionalità, come nell'esempio, premere Enter per proseguire.

SYSLOG SERVER ADDRESS

17. Coyote Linux supporta un ampia gamma di schede Ethernet. Si deve conoscere il nome del modulo del driver Ethernet per ogni scheda Ethernet sul proprio firewall e inserirlo sotto. (Si dovrebbe essere già in possesso di questa informazione se si sono seguite le istruzioni alla voce "Attenzione" all'inizio di questo paragrafo). Per le schede ISA, che probabilmente non si posseggono a meno che non si lavori su una macchina molto vecchia, è necessario aggiungere informazioni IO e IRQ.

```
Enter the module name for your lo-
cal network card: 8139too
Enter IO address (Leave blank for PCI
cards):
Enter IRQ (Leave blank for PCI
cards):
Checking module dependencies...
8139too deps = mii
The default language of the Coyote
Web Administrator
is English. Do you like to configure a
different language ? [Y/N]: N
```

18. Per configurare Coyote Web Administrator per un linguaggio diverso dall'inglese, selezionare Y. Scegliere poi dall'ampio numero di linguaggi disponibili. Lo script per il setup di Coyote costruirà quindi l'immagine del floppy:

```
Building package: etc
Building package: local
Building package: modules
Building package: root
Building package: dhcpd
Building package: webadmin
```

19. Inserire un floppy vuoto nel floppy drive e premere Enter per creare il proprio floppy-disk della distribuzione Coyote Linux:

```
Make sure that you have a floppy in
the first floppy drive
in this system and press enter to
continue...
Formatting /dev/fd0u1440
Double-sided 80 tracks 18 sec/track.
Total capacity 1440 kB
Formatting ... done
Verifying ... done
bin/mkdosfs 2.2 (06 Jul 1999)
Installing boot loader...
Copying files...
cp: omitting directory `floppy/con-
fig'
`floppy/dhcpd.tgz' -> `mnt/dhcpd.
tgz'
`floppy/etc.tgz' -> `mnt/etc.tgz'
`floppy/linux' -> `mnt/linux'
`floppy/local.tgz' -> `mnt/local.tgz'
`floppy/modules.tgz' -> `mnt/modu-
les.tgz'
`floppy/root.tgz' -> `mnt/root.tgz'
`floppy/syslinux.cfg' -> `mnt/syslinux.
cfg'
`floppy/SYSLINUX.DPY' -> `mnt/SY-
SLINUX.DPY'
`floppy/webadmin.tgz' -> `mnt/we-
badmin.tgz'
`floppy/config/coyote.cfg' -> `mnt/
config/coyote.cfg'
`floppy/config/fireloc.cfg' -> `mnt/
config/fireloc.cfg'
`floppy/config/firewall.cfg' -> `mnt/
config/firewall.cfg'
`floppy/config/hosts.dns' -> `mnt/
config/hosts.dns'
`floppy/config/portfw.cfg' -> `mnt/
config/portfw.cfg'
`floppy/config/qosfilt.cfg' -> `mnt/
config/qosfilt.cfg'
`floppy/config/reserve.cfg' -> `mnt/
config/reserve.cfg'
```

20. Una volta creato il floppy, verrà chiesto se si vuole creare un altro floppy disk. Digitare y se si vuole un altro floppy disk e inserire un altro floppy disk per crearlo. Altrimenti, digitare semplicemente n per terminare la procedura.

```
Would you like to create another
copy of this disk [y/n]? n
```

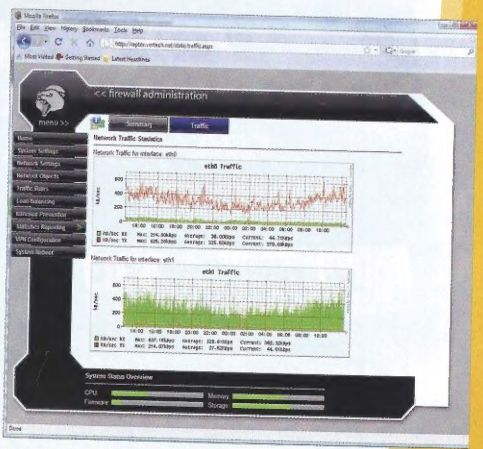
Adesso si è pronti per provare il floppy del firewall Coyote Linux.

COYOTE ALL'OPERA

Per far partire il firewall, basta inserire il floppy disk nel computer di firewall e riavviarlo. Il firewall dovrebbe comportarsi secondo la configurazione che gli si è data. Non c'è nessuna interfaccia diretta con la shell dalla console del firewall, una volta che è partito. In realtà, non è neanche necessario avere un monitor sul firewall perchè comunque non apparirà un prompt di login. Qualsiasi gestione del firewall dovrebbe essere fatta dalla propria LAN.

Se si è configurato il firewall come descritto, il firewall ora:

- Fornisce indirizzi ai computer sulla LAN utilizzando DHCP.
- Lancia una connessione dial-up dal firewall all'ISP non appena qualcuno tenta di accedere ad Internet dalla LAN o dal firewall stesso.
- Autorizza il traffico dalla LAN a Internet.
- Offre servizi di login (sshd) e di amministrazione Web dalla LAN.



La scheda Traffic mostra, attraverso una serie di diagrammi, il traffico di rete.